HUMAN
RIGHTS
CENTER
UC Berkeley School of Law

# DIGITAL FINGERPRINTS

## Using Electronic Evidence to Advance Prosecutions at the International Criminal Court

HUMAN
RIGHTS
CENTER
UC Berkeley School of Law

# DIGITAL FINGERPRINTS

## Using Electronic Evidence to Advance Prosecutions at the International Criminal Court

FEBRUARY 2014

The Human Rights Center at the University of California, Berkeley, School of Law conducts research on war crimes and other serious violations of international humanitarian law and human rights. Using evidence-based methods and innovative technologies, we support efforts to hold perpetrators accountable and to protect vulnerable populations. We also train students and advocates to document human rights violations and turn this information into effective action.

# CONTENTS

# I. INTRODUCTION

**THIS REPORT SUMMARIZES** major points of discussion from the first Salzburg Workshop on Improving War Crimes Investigations, a convening focused on the use of digital evidence to prosecute atrocity crimes (genocide, crimes against humanity, and war crimes). The workshop was held in Salzburg, Austria, from 23–25 October 2013. The Human Rights Center sponsored the workshop in collaboration with CITRIS (Center for Information Technology Research in the Interest of Society), the Office of the Prosecutor of the International Criminal Court, and Salzburg Global Seminar at the Schloss Leopoldskron, an Austrian castle occupied by the Nazis during World War II and subsequently dedicated to promoting human rights and international justice.[1]

The workshop sought to promote an open exchange of ideas and expertise on strategies to improve the capacity of investigators and prosecutors to gather and analyze digital evidence relevant to serious international crimes.[2]

Workshop participants included investigators and prosecutors from the International Criminal Court ("ICC" or "Court"), specialists in cyberinvestigations, human rights investigators, foundation representatives, legal experts, and University of California, Berkeley, faculty and students. (See Appendix A for a list of participants.) While this report presents the major issues discussed at the workshop, parts of the discussion were off-the-record.

The workshop was organized into six sessions:

- *Current Practices and Challenges in Cyberinvestigations* consisted of investigators from the Scientific Response Unit of the Court's Office of the Prosecutor, who are responsible for conducting forensic and digital investigations. Speakers provided an overview of ICC practices with a focus on areas of needed expertise and collaboration.
- *Challenges of Digital Access and Gathering Evidence* comprised experts who discussed legal obstacles to cooperation between the United States government and the Court.
- *Approaches to Digital Access and Gathering Evidence* included experts who discussed recent advancements in the field of cyberinvestigations.

---

1 Humanity United, Open Society Justice Initiative, Open Society Foundations, Sigrid Rausing Trust, and Oak Foundation funded the workshop. Representatives from several of these organizations contributed to discussions.

2 For the purposes of this report, digital evidence is "data that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the proceeding." Stephen Mason, ed., *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

- *Digital Evidence in the Courtroom* drew on the expertise of senior trial attorneys from within and outside the Court. Speakers discussed the unique challenges of incorporating digital evidence in international criminal prosecutions.
- *Probative Value: Evaluating Admissibility* consisted of NGO experts who gather digital documentation of crimes in conflict zones who addressed means of overcoming admissibility concerns.
- *Probative Value and Presentation* included experienced trial lawyers who spoke about the importance of authentication and the presentation of evidence at trial.

To facilitate the discussion, UC Berkeley law students from the International Human Rights Law Clinic and the Samuelson Law, Technology, and Public Policy Clinic presented background papers on relevant topics (See Appendix B). The papers were provided to all attendees in advance.

This workshop is the second in a series of workshops hosted by the Human Rights Center on enhancing evidence collection to support international prosecutions. The first—*Beyond Reasonable Doubt: Using Scientific Evidence to Advance Prosecutions at the International Criminal Court*—helped identify the need to integrate cyberinvestigations into ICC protocols and evidence collection practices. The Human Rights Center will host two additional workshops in 2014. These events will focus on the role of new technologies in investigating atrocity crimes and the development of protocols for non-court actors who gather information to support accountability in the aftermath of such crimes.

# II. BACKGROUND

**SUCCESSFUL PROSECUTIONS** of serious international crimes depend on the collection of a wide range of probative evidence. In the aftermath of atrocities, investigators may be restricted from collecting evidence because of ongoing violence or an inability to access crime scenes. Witnesses may hesitate to come forward, fearing retribution against themselves or their families. Despite these obstacles, investigators can often obtain evidence from a range of digital devices, including computer hard drives, cell phones, photographs, and videos, as well as information posted on the internet. Such digital information can reveal patterns of organized violence and, in some cases, provide evidence linking an accused to the scene of the crime. Investigators are now grappling with how best to collect, analyze, and store this data in order to produce the highest quality evidence.

Established in 2002, the International Criminal Court is a relatively new institution with an ambitious mission. The Court's mandate is to investigate and prosecute the most serious crimes of concern to the international community: genocide, crimes against humanity, and war crimes.[3] To date, the Court has publicly indicted 36 individuals in a total of 21 cases in eight countries. The Pre-Trial Chambers, meanwhile, have dismissed charges against a number of defendants because of a lack of "sufficient evidence to establish substantial grounds to believe" that the accused committed the alleged crimes. Cases against six defendants have advanced to trial; a guilty verdict has been rendered in one case and one defendant has been acquitted.

These prosecutorial setbacks can be attributed, in part, to a lack of quality evidence linking perpetrators to crimes. Considering the Court's global mandate, coupled with its limitations in funding and staff, obstacles to obtaining reliable evidence are unsurprising. In recent years, however, the growing profusion of digital evidence has presented new challenges and opportunities for the Court.

Improving the collection and analysis of digital information can enhance the Office of the Prosecutor's ability to secure quality evidence that results in convictions, as well as diversify evidence coming into the courtroom. The strongest cases are often those in which several different kinds of evidence support the same accounts of the facts. Triangulating multiple pieces of evidence can corroborate witness testimony or authenticate documentary or physical evidence.

Digital evidence can prove particularly useful to prosecutors of serious international crimes. Emails, satellite images, or videos can often provide linkage evidence that ties high-ranking defendants to their triggermen on the ground. Digital evidence can also provide information on the time and place of an event, limit the exposure of vulnerable witnesses, or exculpate those wrongfully accused.

---

3 UN General Assembly, Rome Statute of the International Criminal Court, 2187 UNTS 90 art. 5(1), 17 July 1998.

## Digital Evidence at the International Criminal Court

The Office of the Prosecutor is tasked with collecting and presenting both incriminating and exculpatory evidence in each case before the Court. Evidence must satisfy minimum standards of relevance and reliability to be admitted. The plethora of digital information in the 21st century poses opportunities and challenges. In 2013, for example, the number of mobile phone subscriptions worldwide was reported at 6.8 billion, up from 6.0 billion in 2011, and 5.4 billion in 2010.[4] On the African continent alone, the market penetration of mobile phones hit 65% in 2012, with an estimated 20% annual growth rate.[5] On a continent with few landline phone or internet connections, cell phones are used for communication, social media, and even banking, which means that a considerable amount of personal information and communications may be stored on an individual's phone.

This widespread use of cell phones offers new opportunities to document crimes.[6] Investigators can retrieve emails, phone calls, photographs, videos, banking information, and GPS data from cellular devices. Such data can help court investigators document criminal intent and link perpetrators to specific events, such as massacres, forced displacement, and torture. Digital evidence may also come in the form of social media, such as photographs, video and audio recordings, emails, blogs, and social networking sites (e.g., Facebook, Twitter, YouTube).

Despite the large quantity of digital evidence that may be available and relevant to international criminal cases, collecting and analyzing digital evidence presents a major challenge. A 2013 expert panel, commissioned to review the Office of the Prosecutor's capacity to collect digital evidence, observed, "Digital information is the 'rule rather than the exception' in current investigative activities." Yet, inadequate national cooperation, budget constraints, insufficient software, limited partnerships, an exclusive reliance on keyword searches, and insufficient technological protections to safeguard online anonymity restrict investigators' access to digital information.[7]

Aware of these limitations, the Office of the Prosecutor has made strides toward improving its ability to collect and analyze digital evidence. In 2013, it hired an expert in digital forensics to join its Scientific Response Unit, and sent investigators to trainings on cyberinvestigations held by INTERPOL and other law enforcement organizations. In coming years, it will be important for the Office of the Prosecutor to continue to build its internal capacity through partnerships with governments, law enforcement agencies, NGOs, and technology companies to increase the quality of evidence, build stronger cases, and advance its mandate to prosecute those accused of the world's most grave crimes.

---

4 International Telecommunication Union, *ICT Facts and Figures* (February 2013), available at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf.

5 Peter Lange, "Africa—Mobile Voice and Communications Statistics," BuddeComm (November 2012), at http://www.budde.com.au/Research/Africa-Mobile-Voice-and-Data-Communications-Statistics-tables-only.html?r=51. Market penetration rates vary across the continent. Mobile phones, for example, are more available in Kenya than the Central African Republic. Ibid.

6 See *ICC and Digital Investigation* (2013) (expert report on the capabilities and practices associated with the use of digital investigation and evidence gathering within the ICC Office of the Prosecutor, on file with the authors). See also Tolu Ogunlesi and Stephanie Busari, "Seven ways mobile phones have changed lives in Africa," CNN Website, September 14, 2012, at http://www.cnn.com/2012/09/13/world/africa/mobile-phones-change-africa.

7 *ICC and Digital Investigation,* supra note 6.

## History of Digital Evidence

In the Court's early years, digital evidence did not play a significant role in investigations. Indeed, the Office of the Prosecutor's first major haul of digital evidence took place during the 2008 arrest of Jean-Pierre Bemba Gombo. Bemba, a former Vice President of the Democratic Republic of the Congo and leader of the Movement for the Liberation of Congo, was accused of crimes against humanity and war crimes in the Central African Republic. The Office of the Prosecutor also collected digital evidence during the arrest of Callixte Mbarushimana, a former United Nations employee accused of crimes against humanity and war crimes in the Democratic Republic of Congo. During these arrests, search and seizure procedures produced digital evidence that investigators thought might be useful. But, at the time, the Office of the Prosecutor had no in-house expertise or other technical capacity. As a result, investigators depended on national authorities to collect and process digital information.

By 2011, the Office of the Prosecutor began to investigate cases in which digital evidence was critical, including cases from Kenya, the Ivory Coast, and Libya, where conflicts involved the widespread use of mobile phones, email, social media, and other potential sources of digital evidence. These new cases generated an increased demand for the storage, processing and analysis of digital evidence. In response, the Court began to consider ways to build its relevant capacity.

In 2013, in response to both the prevalence of digital evidence and calls from the judges for stronger evidence, the Office of the Prosecutor embarked on a new strategy focused on open-ended investigations, with the goal of expanding and diversifying evidence collection, and exploiting alternative, non-witness-based evidence-gathering methods. This new strategy included a focus on improving the investigators' capacity to collect and analyze digital evidence and a commitment to creating a Digital Forensics Team within the Scientific Response Unit.

## Digital Evidence in Trial Proceedings

Jurisprudence on the use of digital evidence at international criminal tribunals is limited. What jurisprudence exists reveals that international criminal courts rarely admit digital information as stand-alone evidence. Instead, judges have more commonly considered digital evidence as corroborating evidence, and have admitted it alongside witness testimony or physical evidence.

Judges at international criminal tribunals have tended to prefer witness testimony to digital information.[8] ICC judges, for example, have relied heavily on *viva voce* evidence, recorded testimony or written statements. Yet witness testimony is not without its liabilities. Judge Bruno Cotte, the presiding judge in *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, observed in a 2012 interview that witness testimonies are "often fragile."[9] He went on to say that the Office of the Prosecutor's cases would benefit from diversifying the kinds of evidence it presents at trial. As the Office of the Prosecutor's cases advance further into the 21st century, digital evidence, as a form of non-witness evidence, will become ever more available.

---

8 Rule 69(4) of the ICC's Rules of Procedure and Evidence, ICC-ASP/1/3, states that evidence may be admitted, "taking into account, *inter alia,* the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness." Rule 63(2) gives judges the "authority, in accordance with the discretion described in article 64, paragraph 9, to assess freely all evidence submitted in order to determine its relevance or admissibility."

9 Franck Petite, "Interview with ICC judge Bruno Cotte, presiding judge at the second trial at the ICC," Radio Netherlands Worldwide, 20 June 2012, available at http://www.rnw.nl/international-justice/article/judge-cotte-%E2%80%9Cwe-are-making-progress%E2%80%9D.

Yet introducing digital evidence into the courtroom has its challenges. Digital information, such as photos and videos, must be verified and authenticated and chain of custody must be established. Because online sites such as YouTube strip the metadata—e.g., information about when and where a video was filmed—it is often difficult to establish probative value.

Despite these limitations, the Office of the Prosecutor has begun to introduce more digital evidence in proceedings. For example, a video was one of the key pieces of evidence used to convict Thomas Lubanga, the Court's first defendant, of conscripting children to fight in Eastern Congo.[10] The video portrayed Lubanga inspecting troops with boys and girls in military fatigues. The prosecution also successfully introduced into evidence ten audio recordings of radio broadcasts in another case, despite challenges from the defense regarding their authenticity. Such recordings provided background information about the conflict, the identity of those involved, as well as accounts from eyewitnesses and victims.[11]

ICC judges have also resisted admitting digital evidence. For example, in November 2013, judges in *The Prosecutor v. William Samoei Ruto and Joshua Arap Sang* declined to admit recordings of a radio program hosted by Sang, holding that the source of the recordings was not clear. According to the *Kenya Monitor*, "judges would only allow those particular recordings to be marked for identification. This means they will be in the court records but will not be part of the evidence the judges will weigh to reach a verdict in the case against Sang."[12]

Legal challenges, however, to recent video and broadcast recordings may pale in comparison to future court disputes, given the growing prevalence of social media (e.g., Facebook and Twitter), photo and video sharing sites (e.g., YouTube, Flickr, and Instagram), and smartphone proliferation in less stable states. Such digital evidence offers tremendous opportunities for prosecutors to strengthen cases by presenting such information in trials.

---

10 See Prosecutor v. Lubanga (Judgment), ICC-01/04-01/06, para. 1244 (14 March 2012).

11 Prosecutor v. Bemba, *Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute,* ICC-01/05-01/08 (27 June 2013).

12 International Criminal Court Kenya Monitor, "Judges decline to admit into evidence some recordings of program Sang hosted," 5 November 2013, at http://www.icckenya.org/2013/11/judges-decline-to-admit-into-evidence-some-recordings-of-program-sang-hosted.

# III. MAJOR ISSUES

**THE NUMBER, SCALE, AND GLOBAL REACH** of current and future investigations dictate that the International Criminal Court must make progress building its in-house capacity; however, collaboration with external partners will also be essential. Put simply, the Court cannot develop a cyberinvestigation program capable of handling vast case loads and still remain abreast of cutting-edge technological developments. As representatives of the Office of the Prosecutor explained at the Salzburg Workshop, it is imperative that a plan for the next 10 years be put in place to better gauge where technological innovations are heading and to forge partnerships with leading technology specialists.

## Building the Court's Internal Capacity

The Office of the Prosecutor recognizes that its cyberinvestigation capacity lags behind many national jurisdictions. During the Office of the Prosecutor's initial encounters with digital evidence, all of the collection, processing, and initial analysis was outsourced, usually to national law enforcement bodies. However, as one ICC staff member pointed out, outsourcing has its drawbacks. National authorities must prioritize their own cases and thus have limited time, staff, and resources to offer the Court during its lengthy investigations. Moreover, the Office of the Prosecutor is often limited in the amount of information it can provide to outside experts about specific cases due to confidentiality and procedural concerns. The national experts processing the digital evidence may not have sufficient background on the offenses, an understanding of their context, or even know what information to look for during their analysis.

In recent years, the Office of the Prosecutor has improved its ability to extract and analyze digital information on hardware devices such as computers and mobile phones. Investigators are just beginning to build their own software and hire personnel. They are currently able to duplicate and analyze hard drives. Working with mobile phones, investigators can now conduct more advanced analysis in-house. However, major challenges remain. First, some phones are difficult to analyze with the Office of the Prosecutor's existing equipment. Additionally, newer, more sophisticated mobile phones may contain valuable sources of information, such as emails and browser histories, which can be difficult to capture without specialized techniques and software.

Over the past six months, the Office of the Prosecutor has begun to hire additional staff and build partnerships with outside technology companies in an effort to improve its ability to conduct "online investigations"—that is, the retrieval of digital evidence divorced from a hardware device. However, to truly build this capacity, the Office of the Prosecutor will need to invest in new software and computers to conduct secure,

anonymous, and effective digital investigations. It will also need to revise investigation protocols to address the need for gathering and analyzing more current forms of digital evidence.

The Office of the Prosecutor recognizes that its capacity to conduct cyberinvestigations falls well below the standards set by many leading technology companies. The Court, for example, lacks dedicated internet lines and offline storage capacity designed to insulate investigations from other court activities. Investigators also lack online anonymity, currently receive limited training on security and best practices, and have no comprehensive standard operating procedures (SOPs). These deficits highlight the need to develop the Court's in-house capacity, protocols, and procedures in order to conduct more secure and effective investigations.

As the Office of the Prosecutor strengthens its ability to gather and analyze digital evidence, it must also develop SOPs to instruct investigators on how to handle evidence in an appropriate manner. Some of this will require internal decisions, such as whether to train field investigators in digital forensic techniques or hire specialized staff. Field investigators generally know their cases better than cyberinvestigation specialists. They have a good idea of the relevant country's situation, culture, history, and language. Still, field investigators have many priorities, and long-term training and oversight on digital investigations may prove impractical.

The expert panel commissioned to assess the Office of the Prosecutor's cyberinvestigation capacity has concluded that more resources are needed for staffing, equipment, and training—a conclusion underscored during the workshop. A lack of resources is the greatest constraint on the Office of the Prosecutor's ability to produce quality digital evidence. Digital investigations require expensive equipment and up-to-date software licenses, and funding to create a dedicated digital investigation unit and provide regular training. In particular, the panel recommended the establishment of a Digital Forensics Team, which would be able to determine the Court's specific software and hardware needs.[13] Once internal decisions such as personnel allocations are made, the Office of the Prosecutor will need to provide regular training to ensure that investigators' technological expertise remains up to date. This will likely require the Court to partner with more experienced actors in the field of cyberinvestigations both for the expertise and to defray costs.

## Fostering External Partnerships

The Office of the Prosecutor can look to many organizations for guidance as it continues to develop its ability to collect and analyze digital evidence. National law enforcement, as well as transnational bodies such as INTERPOL, have considerable experience collecting and analyzing digital evidence, and may be able to assist the Court as it develops its capacity to do the same. Nongovernmental organizations (NGOs) working with witness video and photographs could be innovative partners, and technology companies could assist with expertise, hardware, and software.

Government agencies in the United States, such as the Federal Bureau of Investigations (FBI) and the Department of Homeland Security (DHS), have units dedicated to cyber crimes and have developed considerable expertise in online investigations. Agents are experienced in all types of forensics and frequently use their specialized skills to support field operations. The Court should seek permission to work with these agencies by making official requests through diplomatic channels.[14]

---

13 *ICC and Digital Investigation,* supra note 6.

14 While the ICC can learn much from the expertise and the examples of international and interagency cooperation utilized by US government agencies, there are serious barriers to official cooperation with the United States. The American Servicemembers'

In addition, the FBI has pioneered a series of international partnerships to facilitate the collection of digital evidence. These partnerships allow FBI special agents to be stationed in national police jurisdictions across Europe, where they work directly with their domestic police counterparts. This streamlines international cooperation and speeds information sharing.

The ICC could also expand its work with INTERPOL, the International Criminal Police Organization, based in Lyon, France. The organization has considerable capacity to support investigations of serious international crimes and is building a new location in Singapore dedicated to cyberinvestigations and cybercrime. In addition, INTERPOL runs the Strategic Alliance against Cybercrime, which provides digital training courses and other services to support the efforts of member countries. INTERPOL also assists countries in the coordination of joint operations, including forensic support and access to forensic labs.

NGOs that collect and analyze videos and photographs produced by citizen witnesses may also make strategic partners. Several NGOs are developing new strategies to address authentication and chain of custody issues. A handful are providing tools in the form of "apps" that citizen witnesses, who are often already filming and photographing abuses, can use to ensure retention of important information, including when and where a video was filmed. These apps record geolocation, nearby cell towers, pitch, roll, light meter readings, and device identity, facilitating authentication. Additionally, some apps allow users to upload photographs or videos to secure servers to preserve a copy of the original data and establish chain of custody, while still allowing the user to post or otherwise distribute a copy of the recording for non-court purposes, or erase it from the device entirely.

Other NGOs have adopted a different approach. Rather than capitalizing on existing citizen witnesses, they provide cameras to citizens in conflict zones and offer training on covert filming, security, and chain of custody to help them record abuses that might otherwise go undocumented. These videos could then be aggregated and displayed in a browser simultaneously; multiple independent accounts of a single event would strengthen their probative value and reduce the likelihood of accusations of fraud by the defense. Both of these approaches are sophisticated front-end tactics that can improve the quality of digital evidence available to the Office of the Prosecutor. The Human Rights Center's Workshop in Salzburg provided an opportunity for Office of the Prosecutor staff and NGO representatives to explore how mutually beneficial partnerships could be formed.

Cooperation with NGOs that are already collecting digital evidence in the form of photographs and videos offers a compelling opportunity to expand the reach of the Office of the Prosecutor. As one Court staff member said, "Lawyers are not innovators. They are traditionalists by nature." In contrast, NGO investigators tend to be innovators, often experimenting with new technologies and approaches.

Cooperation between NGOs and court prosecutors poses challenges, however. NGOs have their own motivations and mandates, which may not include producing court-admissible evidence. A platform is needed through which the Court can easily interact and discuss ideas with NGOs. An NGO representative suggested that something as simple as a link on the ICC website that provides instructions as to how NGOs should submit evidence would be a first step toward building effective partnerships.

Relationships with private technology companies may also help the Office of the Prosecutor keep abreast of technological advancements and defray the costs of necessary software and hardware. Technology

---

Protection Act (ASPA), signed into law in 2002, prohibits any US government agency from assisting the ICC in a way and forbids any ICC investigative activity in the United States. The ASPA does contain limited exceptions, including the Dodd Amendment, which allows for US cooperation with ICC prosecutions of foreign nationals on a case-by-case basis.

engineers often have philanthropic interests, and may be willing to assist with the Court's mission of promoting global justice. Meeting with independent programmers may be a way to galvanize support for the Court and build a network of innovative assistance without incurring prohibitive costs.

Workshop participants also discussed the extraordinary benefits that could come with collaboration between the Court and large technology companies such as Yahoo!, Microsoft, Google, Facebook, YouTube and others. These companies hold much of the world's digital data and as private entities may not face the same restrictions on ICC cooperation as government agencies.

# IV. RECOMMENDATIONS

**THE ABILITY TO COLLECT** and analyze digital evidence is growing in importance for the International Criminal Court. Based on discussions at the workshop, we recommend 1) greater investment in the Court's internal capacity to collect and process digital evidence; 2) an increased effort to develop relations with external partners, such as governmental agencies, nongovernmental organizations (NGOs), university research labs, and technology companies; and 3) ongoing dialogue on the ways that new technologies can advance ICC prosecutions.

## Investing in the Court

*Hire Specialists in Digital Evidence* — The Office of the Prosecutor should hire specialists trained in advanced cyberinvestigation techniques and familiar with cutting-edge technologies. In the hiring process, the Office of the Prosecutor should emphasize experience and credentials specific to digital investigations, including computer and smartphone forensics, online investigations, data storage and management, advanced cyberinvestigation techniques, and superior knowledge of digital security. Bringing on specialists in digital data mining and analysis will go a long way toward building a robust in-house capacity for vetting digital data and extracting quality evidence.

*Develop Internal Protocols* — The Office of the Prosecutor should develop comprehensive internal protocols to govern gathering and handling digital evidence. Ideally, the Office of the Prosecutor should hire individuals who have backgrounds developing or working under precise cyberinvestigation protocols in top security posts. These individuals can lead the way in the implementation of consistent and modern protocols across cases and help to assure that digital forensic analysis at the Court complies with the most up-to-date standards. These new protocols should reflect best practices used by other top cyberinvestigations units worldwide.

*Invest in Training* — The Assembly of State Parties of the International Criminal Court should invest in ongoing training for current and future investigators in the Office of the Prosecutor. Technologies change rapidly. It is vital that the Court's cyberinvestigation capacity keep pace. The Court has demonstrated a willingness to invest in training and partner with other cyberinvestigation organizations. A continued commitment to such collaborations is essential.

*Update Technologies* — The Office of the Prosecutor should stay abreast of new technologies and techniques for collecting and analyzing digital data. Similar to ongoing trainings for staff, updating technology will

be necessary to preserve the capacity of investigation teams to properly handle and evaluate digital data. Partnerships with leading technology firms or university researchers could help ensure the systematic and continuous incorporation of emerging software and hardware at the Court.

### Fostering External Partnerships

*Partner with NGOs* — The Office of the Prosecutor should reach out to NGOs that specialize in gathering digital evidence as potential partners, and communicate how they might assist the Court should they wish to do so. A number of NGOs have developed innovative methods to gather digital evidence. Such groups are well positioned to aid the Court with various court-specific challenges, such as authentication. Further, such NGOs have extensive networks within the technology sector, and could provide introductions to key players in the world of cyberinvestigations. NGOs also frequently work closely with civil society organizations, citizen journalists, and locals on the ground who could assist the Court in obtaining digital information or authenticating evidence. In particular, the Office of the Prosecutor should seek out partnerships with NGOs specializing in the digital documentation of violence, especially those working in ICC situation countries. These organizations have expertise related to the collection of digital data and also the requisite understanding of the paramount importance of security with relation to investigations of atrocity crimes.

*Partner with International Investigatory Organizations* — The Court should cultivate stronger partnerships with international organizations. In particular, it should explore the scope of its cooperation agreement with INTERPOL, and make use of available *services, training, and outreach capabilities*. INTERPOL can assist ICC investigators by locating relevant digital evidence in one or more member countries, facilitating the processing of formal request for cooperation through its network of experts in digital crime and war crimes, enabling the transmission of the evidence through its secure communication network, and providing trainings in cyberinvestigations.

*Partner with Technology Companies* — Large technology firms have significantly more resources, staff, and expertise to dedicate to keeping abreast of new technologies than the Office of the Prosecutor and, if so inclined, could provide valuable assistance to offset costs of cyberinvestigations. In particular, we recommend the Court build relationships with leading companies, such as Microsoft, Google, Facebook, and Yahoo!, which have established philanthropic arms and may be well positioned to support the Court. Such technology firms could also aid the Court with innovation and security.

*Partner with Computer Science Researchers, Programmers, Developers, and User Experience Experts* — The Office of the Prosecutor may also want to consider relationships with independent technology specialists in order to capitalize on their insights and expertise. Within the technology sector, innovation often emerges from individuals or small collectives, like university research labs, working on specific problems. In some instances, it may prove advantageous for the Court to partner with third-party organizations or universities to sponsor hackathons or similar events devoted to solving its technical challenges.

*Partner with Government Agencies* — The Court should explore working with State Parties' investigatory agencies and be more active in making individual requests for cooperation on a case-by-case basis, as permitted by the Rome Statute and national legislation. The Court could benefit from their expertise. While the extent and depth of potential cooperation with each state is unclear, the ICC has little to lose by making

specific requests through proper diplomatic channels. The Court could also seek cooperation with Non-State Parties, when those governments have particular expertise related to specific cyberinvestigations.

## Continuing Conversations

*RightsCon* — Workshop participants discussed opportunities to expand interactions between the ICC and technology firms. By building partnerships with leaders in the technology sector, the Court can take advantage of research and development within those companies, and keep investigators apprised of the newest technologies and techniques for conducting cyberinvestigations. Technology firms may also be willing to provide free copies of new software or work with ICC staff to adapt technologies to the Court's needs. To that end, the Human Rights Center and Videre will convene a daylong workshop as part of the RightsCon conference in San Francisco in March 2014. The workshop will bring together representatives from Silicon Valley technology companies, the Office of the Prosecutor, and NGOs working at the nexus of digital documentation and human rights to discuss future collaboration and cooperation. The Human Rights Center and Videre will also coordinate a public "scrum" at RightsCon to foster lively debate among leading human rights advocates and technology leaders about the tensions between privacy, security, and the need for access to information to facilitate digital investigation of atrocity crimes.

*Salzburg Workshop on Field Methodologies* — Building on discussions at the workshop, the Human Rights Center will also convene a second Salzburg workshop in September 2014 that focuses on field methodologies for ICC partners working in conflict zones. Local NGOs and other non-court actors—journalists, aid workers, and human rights researchers—often witness atrocity crimes and other human rights violations or arrive soon after they occur. They are well positioned to gather evidence, including digital evidence, which can be useful to ICC prosecutors. Yet, many organizations and individuals working in ICC situation countries lack knowledge about how to properly collect and handle material to ensure that it can be authenticated and thus used in court. Failures to preserve information on chain of custody and other details may not be correctable later. To address these issues, the Human Rights Center will bring together court and non-court actors, including representatives from human rights organizations and NGOs working in conflict zones around the world, to discuss best practices for investigations, develop pragmatic approaches for sharing digital information, and draft guidelines to improve the reliability and admissibility of potential evidence.

# Appendix: Workshop Participants

## Chairpersons

CAMILLE CRITTENDEN, Deputy Director, CITRIS: Center for Information Technology Research in the Interest of Society, University of California, Berkeley

ERIC STOVER, Faculty Director, Human Rights Center and Adjunct Professor of Law, School of Law, University of California, Berkeley

## Participants

JEAN-JACQUES BADIBANGA, Trial Lawyer, International Criminal Court

WENDY BETTS, Director of the eyeWitness project, International Bar Association

JEFF BRANNIGAN, National Program Manager, Cyber Crimes Center, US Homeland Security Investigations (HSI)

JULIE BROOME, Head of Human Rights, Sigrid Rausing Trust

STEPHEN CODY, Director, Atrocity Response Program, Human Rights Center, School of Law, University of California, Berkeley

YVAN CUYPERS, Cyberinvestigator, Office of the Prosecutor, International Criminal Court

JENNIFER EASTERDAY, Trial Monitor and Consultant, Open Society Justice Initiative

ALEXA KOENIG, Executive Director, Human Rights Center, School of Law, University of California, Berkeley

LAUREL E. FLETCHER, Clinical Professor of Law, School of Law, University of California, Berkeley

JACQUELINE GEIS, Head of Development and External Relations, Videre

MARTIN KOSTOV, Administrator, Fugitive Investigative Support Sub-directorate, INTERPOL General Secretariat

TIM LICENCE, Creative Director, International Bar Association

STEPHEN MASON, Barrister, Institute of Advanced Legal Studies

PEGGY O'DONNELL, Researcher, Human Rights Center, School of Law and PhD Candidate, Department of History, University of California, Berkeley

BORISLAV PETRANOV, Senior Advisor, Human Rights Initiative, Open Society Foundations

CRISTINA RIBEIRO, Investigation Coordinator, Office of the Prosecutor, International Criminal Court

BETH VAN SCHAACK, Professor, University of Santa Clara School of Law and former Deputy to the Ambassador-at-Large for War Crimes Issues in the Office of Global Criminal Justice of the U.S. Department of State

PHIL SLINKARD, Special Agent, United States Federal Bureau of Investigation (FBI)

JENNIFER M. URBAN, Assistant Clinical Professor of Law and Director of the Samuelson Law, Technology and Public Policy Clinic, School of Law, University of California, Berkeley

VIOLA VIEDERPASS, Digital Crime Officer of Cyber Innovation and Outreach, INTERPOL Global Complex for Innovation

OREN YAKOBOVICH, CEO, Videre

SABINA ZANETTA, Forensic Officer, Office of the Prosecutor, International Criminal Court

### Rapporteurs

AIDA ASHOURI, Law Student, School of Law, University of California, Berkeley

CALEB BOWERS, Law Student, School of Law, University of California, Berkeley

CHERRIE WARDEN, Law Student, School of Law, University of California, Berkeley

2850 TELEGRAPH AVE., SUITE 500
BERKELEY, CA 94705-7220
PHONE: 510.642.0965
EMAIL: HRC@BERKELEY.EDU
HRC.BERKELEY.EDU
HRC.BERKELEYLAWBLOGS.ORG