2014/SOM1/ACT/012
Agenda Item: 10

Handbook (First Part) - Best Practices in Investigating and Prosecuting Corruption Using Financial Flow Tracking Techniques and Financial Intelligence

Purpose: Information
Submitted by: Chile

**18th Anti-Corruption and Transparency
Experts' Working Group Meeting
Ningbo, China
20 February 2014**

Asia-Pacific
Economic Cooperation

Best Practices in Investigating and Prosecuting Corruption Using Financial Flow Tracking Techniques and Financial Intelligence

A Handbook
First Part

APEC Anticorruption and Transparency Working Group
(ACTWG)

November 2013

TABLE OF CONTENTS

PRESENTATION

The following pages constitute the first part of a handbook that will be completed and published by 2015. This handbook was elaborated under the scope of APEC project M SCE 01 12A-1: “Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration”.[1] The project was borne within the APEC Anticorruption and Transparency Working Group (ACTWG), from joined efforts made by Chile and Thailand to improve corruption and money laundering investigation and prosecution. Both economies, members of the APEC ACTWG, will be leading the project under the Multi Year Project APEC Guidelines, through 2013 to 2015.

This multi-year effort has been designed in two subsequent stages.

The first one, led by Chile, consisted in the revision of the legislative and regulatory framework of investigating and prosecuting corruption and the laundering of its proceeds of 10 APEC economies: Australia; Canada; Chile; Indonesia; Hong Kong, China; Malaysia; Mexico; Peru; The Russian Federation; and The United States. Those economies – with the exception of Canada –, plus Brunei Darussalam; Chinese Taipei; The Republic of the Philippines; and Viet Nam participated in a three-day workshop “Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration”, that took place in Santiago de Chile from June 11 to June 13, 2013. During the workshop, the economies presented and discussed their best practices for investigating and prosecuting corruption and the laundering of its proceeds.

The proposed objectives of the workshop were to focus the presentations on financial investigation techniques and on the use of digital forensics for uncovering corruption. The presentations, however, also brought to the table other important issues in investigating corruption, such as the essential elements of building of an investigation plan and strategy and the best practices related to building coordination mechanisms and cooperative networks both domestic and internationally.

The following pages capture the knowledge gained from the workshop, including the content of the presentations and discussions developed therein.

We start by introducing the basics of any investigation: how to develop a plan, how to organize the resources, identify potential targets, define the scope of the investigation and select the techniques that will be used to potentially prove the allegations (Chapter I).

Chapter II focuses on issues of coordination, both domestic and international, and in the related aspect of building cooperative networks. We review the best practices for domestic cooperation, taking into account the internationally recognized practices for sharing information, especially financial information. In light of the workshop discussions, we specifically revisited the coordination between FIUs and other law enforcement agencies.

While Chapter III focuses on the gathering of peripheral evidence, through open sources techniques, databases searches, and digital forensics tools, Chapter IV explains the gathering of private sources of evidence, including the use of digital forensic tools. Chapter V closes this first part of the handbook, with a practical approach on how to perform human intelligence, specifically the technique of profiling suspects.

The second part of the handbook is envisaged as, on the one hand, completing the evidence gathering chapters, mainly by focusing on the gathering of financial evidence. On the other hand, it is suggested that the second part of the handbook develop three chapters devoted to the asset recovery process: restraining measures, confiscation proceedings and repatriation issues. This second part will be built through a similar process than the first part: in 2014, led by Thailand, a workshop to share best practices in financial evidence and asset recovery best practices will serve as a basis for writing those remaining chapters.

CHAPTER I: PRE-CONDITIONS FOR CONDUCTING COMPLEX INVESTIGATIONS

Investigations of corruption are often very complex, since they usually involve a multitude of relevant actors and targets, movement of assets and financial vehicles used or placed in overseas jurisdictions. Successful investigations of complex corruption schemes are not only the result of dedicated individual efforts but also the consequence of some institutional pre-requisites, which provides an adequate environment for such a success to take place.

This introductory Chapter is devoted to remind the essential pre-conditions that any competent authority needs to envisage as the ideal grounds for ensuring the success of complex investigations and, to the extent of its responsibilities, help to build the institutional capacities towards its fulfillment.

The primary objectives of an investigation are:

- Evidence gathering
- Fact finding and reconstruction
- Reporting to / supporting conclusions of the competent authorities.

The investigative team's main responsibility is to bring facts to life for prosecutors, judges and other competent authorities with decision-making capacities. Investigations should be capable of providing grounds to both criminal prosecutions and to the reorganization of public or private administrations with the purpose of preventing the same facts from happening again.

The first step of an effective investigation is its planning. Investigators should begin by identifying the standards, rules, and procedures that govern the circumstances under investigation and the information already available. They must determine what additional information will be required before findings and recommendations may be made to the competent authority, and therefore should elaborate an understanding of the steps which are required to obtain the necessary evidence, including, among others, a list of potential sources of information and specific strategies for witnesses interviewing, in order to reach a conclusion on the merits. The plan should also try to anticipate possible factual and legal challenges and build a case to avoid them.

A policy document including a clear description of the facts that gave rise to the investigation, existent evidence and strategies for gathering additional information, as well as all decisions made in the different investigative stages, along with their justification, is a helpful tool for the investigative team to plan the different steps of the investigation and progressively re-evaluate such plans against evolving developments in an ongoing manner.

The key elements of an investigation plan are the following:

A. Ensuring adequate resources

Before starting an investigation it is important to properly evaluate the necessary resources that will be necessary to complete the task. A comprehensive list of all the needed resources for the investigation to be successful -either human, financial or material-, is a relevant initial step to organize the investigative work from the beginning.[2]

Basic items to be factored in are whether and what types of internal and/or external expertise should be involved with the investigative team; the special investigative techniques that will be required and their potential costs; whether interagency cooperation/coordination will be necessary, and appropriate paths to ensure it, including the use of international legal or operational cooperation, information exchange and possible travel; and the usefulness of establishing joint investigative teams.

As many member economies recognized, from the onset of any investigation particular consideration should be given to the necessary expertise to trace financial flows and other illicitly acquired assets, especially when other jurisdictions are identified as potential recipients of the proceeds of the crime.

Finally, it is also essential to ensure the confidentiality of the investigation and its products and, in turn, evaluate whether the systems for the creation, retention and analysis of records fulfill this condition.

B. Building an investigation team

1. Team selection

The selection of an effective team is crucial to the success of an investigation. Team members should possess specific investigative skills likely to be needed in the investigation. An increasing number of member economies are aware of the need to ensure an adequate number of properly trained financial investigators, in addition to more traditional field or legal investigators.

Necessary skills to conduct large-scale corruption investigations include financial investigations and information technology skills, knowledge of international conventions, standards, and international cooperation mechanisms, undercover and surveillance operations specific expertise, proper experience in interviewing and witness preparation, and the ability to analyze intelligence. Report writing capacities are also essential.

Team members must be aware of all the implications of the investigation, particularly when undercover work is to be conducted.[3]

Finally, it is also essential that the integrity of the team members is absolutely ensured and, to this end, the background of investigators should be thoroughly checked, including social and family ties and lifestyles.

2. Team training

Adequate training and resources for investigators are necessary to ensure that reported cases are dealt with effectively; the wide range of corruption types requires an equally wide range of skills and knowledge on the part of investigators.

Training and education programs should be standardized within each competent authority. Basic training should be envisaged at entry level, and specialized training on select officers should be conducted at both entry level and throughout the investigator's career. Investigators' training may also be aligned with training for specialist prosecutors and other relevant enforcement authorities.

It has been internationally advised that the formal selection of the investigation team members should be followed by formal instruction in at least three primary disciplines: financial intelligence, evidence gathering, and asset tracing/freezing. Further training should be given for purposes of money laundering investigations, enhanced financial intelligence, and criminal and non-conviction based confiscation.[4]

Since these investigations are usually complex and lengthy, financial investigators, intelligence analysts and other authorities should be trained in how to periodically document their findings and in the skills of report writing. Reports are an integral part of financial investigations: the ability to convey concepts, findings and conclusions in a clear, concise and informative manner is essential to their success and therefore it is highly advisable that member economies dedicate the necessary resources to this end.

Where possible, training should not be exclusive to law enforcement but also include such sectors that are required to report suspicious or risky activity. It may also include multiple jurisdictions in order to allow for best practices sharing, learning comparative models and enhancing co-operation. Besides, investigators should remain vigilant in staying current to new trends and typologies. To such ends, APEC economies should encourage their investigators to attend regional and international training workshops with their foreign counterparts.

For example, Chile's Specialized Anticorruption Unit (*Unidad Especializada Anticorrupción* – UNAC) organizes periodic training activities coordinated by specialized lawyers who educate and update prosecutors, investigation agencies and other actors on anticorruption and financial investigations.

3. Engaging specialized experts

Most times, the availability of enough skilled and trained investigators depends on whether enough resources are available for law enforcement. As resources are usually limited, training investigators in the sophisticated techniques needed to deal with the complexities of large-scale corruption cases represents a particular challenge. In such scenarios, engaging experts is convenient to enhance the team's level of expertise.

Specialized experts can play a significant role in financial investigations, e.g. regarding financial analysis, forensic accounting, and computer forensics. Experts use IT tools for tracking and analyzing data and other evidence, and explain transactions or how specific industries or business work.

In particular, assistance of forensic accountants should always be available to the financial investigation team: an opinion derived from a forensic test may help to obtain additional information or may provide closure to other areas of the inquiry, assist in tracing transactions back to the money or assets, provide full analytical review of money flows, identify unexplained transactions, match employees lifestyle with predicted income, or establish links between related parties.

There are various models of drawing on specialized expertise. In some member economies, anti-corruption investigation and prosecution authorities try to build-up their own in-house expertise on specific subject matters, like the US Department of Justice does with forensic accountants or Chile with their in-house financial analysts. Other countries, often those of more limited resources, opt for the involvement of external expertise or a combination of the two approaches. When engaging private entities, however, adequate safeguards should be in place to minimize the risks of compromising the integrity of investigations.

C. Identifying potential targets

Embezzlement of public funds and corruption cases always involve personal gains. From the criminal perspective, an important part of keeping the crime uncovered is to bring satisfactory benefits for all those included in the scheme, in order to ensure their commitment to secrecy. Therefore, in order to identify potential targets of the investigation it is important to “follow the money” or other forms of gain or benefits, and determine who profited from the corrupt act and how. To such end, the following suggestions should be taken into account: [5]

- Tax returns, financial disclosure forms, employment records, and loan applications should be reviewed;
- Immediate superiors and fellow employees are usually good sources of information (suspects have a way of revealing themselves and their processes to those they associate with on a daily basis);
- Public registries, credit card accounts, expensive celebrations, school fees and support measures for children, foreign bank accounts, homes and second houses and holiday homes should be located and assessed, as well as means of transport and employees salaries and perks;
- Even at these preliminary stages, experts should be on hand for consultation, even at an informal fashion. Document examiners, for example, can be consulted for handwriting examinations, signatures, paper and ink analysis and comparison, erasures or substitution of documents, and restoration of obliterated writing. Fingerprint experts, experts in computers and cybercrimes (e-commerce fraud, stenography analysis, data recovery, etc.) and experts in DNA testing (for intimate contact items, such as used stamps and envelopes) may be of great help.
- Once a particular suspect has been identified (or grounds for suspicions arise), the screening process should include persons with whom they have strong ties (family members, business associates, etc.) considering that bank accounts, real estate, land or stocks are often in the names of people of the suspect’s trust.

D. Developing an investigative strategy

1. Case selection strategies

Given the extent of corruption, the range of cases likely to exist, the variety of possible outcomes, and the limits imposed by human and financial resources constraints, most anticorruption law enforcement agencies will find it necessary to make priority choices as to the cases to pursue, and the outcomes to seek. In practice, it must be recognized that not every suspected case can be fully investigated and prosecuted.

Moreover, as it has been widely recognized, detecting corruption involves a key problem in itself. Although decidedly not a “victimless” crime, many crimes of corruption, particularly bribery and trading in influence, are consensual crimes and therefore complainants are hard to find. Furthermore, as corrupt deals usually occurred without witnesses, rarely are documented and are normally surrounded by secrecy, few overt occurrences are likely to be reported by witnesses, unless they are “insiders”. The importance of intelligence in the pro-active detection of corruption therefore stands out. Anticorruption agencies that only rely on re-active strategies, are usually overloaded by thousands of small cases which, coupled with inappropriate case-management techniques, transform them in heavily bureaucratic agencies with the obvious lose of social legitimacy in the long run[6].

Even though it is usually delimited by law or by specific agency guidelines, prioritizing involves the exercise of considerable discretion, so it must be managed carefully to ensure consistency, transparency and the credibility of both the decision-making process and its outcomes. A major element in this regard is the setting and, where appropriate, the publication of criteria for case selection (sometimes referred to as a prosecution policy paper). This document can help reassure those who make complaints, as well as the general public that a decision not to pursue a particular reported case is based on objective criteria and not on improper motives.

Case selection criteria should include the following:[7]

- **The seriousness and prevalence of the alleged offense**

Assuming that the fundamental objective of an anti-corruption strategy is to reduce overall corruption, priority may be given to cases that involve the most common forms of corruption. Where large numbers of individuals are involved, or structural practices are targeted, the case will often lead to proactive remedial outcomes such as the setting of new ethical standards or the training of public officials, general preventive policies with large-scale remedial capabilities.

On the other hand, as overall expertise and knowledge are gained and greater numbers of cases are dealt with, intelligence information can be gathered and assessed, constituting a useful tool for prioritizing cases on the grounds of their seriousness. Intelligence should guide case selection decision making processes through the detection of overall corruption patterns and the identification of such cases which are causing the most social or economic harm.

- **Related cases in the past to establish precedent**

Priority can be given to cases that raise social, political or legal issues the results of which can be applied to many future cases. Examples include dealing publicly with common conduct not hitherto perceived as being corrupt in order to change public perceptions, and cases that test the scope of criminal corruption offences so that either set a useful legal precedent or establish the need for legislation to close a legal gap.

- **The viability or probability of a satisfactory outcome**

Cases may be downgraded or deferred if an initial review establishes that no satisfactory outcome can be achieved. Examples include cases in which the only desirable outcome is a criminal prosecution but it may not be possible or in the public interest to prosecute (i.e. the suspect has died or disappeared, is already serving a lengthy term in prison, is extremely old or critically ill) or where essential evidence has been lost. The assessment of such cases should include a review of whether other appropriate remedies may be available.

- **The availability of financial, human, and/or technical resources to adequately investigate and prosecute**

The overall availability of resources is always a concern in determining how many cases can be dealt with at the same time or within a given time period. An assessment of costs and benefits before decisions are made is thus important. In cases of grand corruption and with transnational implications there can be substantial costs in areas such as travel and foreign legal services, but the public interest may demand that examples are made of corrupt senior officials for reasons of deterrence and credibility, to recover large proceeds hidden either at home or abroad and to restore faith in government.

A periodic reassessment of caseloads is required, since the burden of particular cases tends to fluctuate as investigations proceed. A single major case, if pursued, may result in the effective deferral of large numbers of minor cases, and the unavailability of specialist expertise may make specific cases temporarily impossible to pursue.

- **The legal nature of the alleged corrupt activity**

Corruption can give place to either criminal or administrative/civil procedures. The nature of the offence will often determine which agency is competent to deal with it. The possibility of initiating action other than a prosecution, if circumstances allow, should be considered taking into account the criteria here referred to and the prosecution agencies workload, among other factors.

2. Case management

Member economies should be proactive in developing effective and efficient strategies to make financial investigations an operational part of their law enforcement efforts. Although some corruption cases may be simple and straightforward, with witnesses and evidence readily available,[8] in most cases –especially where corruption is systemic–, the challenge is one of volume. Serious corruption investigations, particularly those involving high-level or grand corruption, can be highly time-consuming, complex and expensive.

To ensure the efficient use of resources and successful outcomes, the investigative tools and personnel involved must be managed effectively. The work of the investigative team should be conducted in accordance with an agreed strategy and supervised by an investigative manager in charge of receiving information about the progress of investigators regularly.[9]

Key elements that will facilitate case management include:

- Periodically conducting needs assessments and promoting proper allocation of resources.
- Articulating clear objectives for relevant departments and agencies that include effective coordinating structures and accountability.
- Establishing strategic planning working groups to develop an effective policy that incorporates the skills of all relevant agencies into an action plan; these groups should include representatives from all relevant agencies and components participating in financial investigations.
- Creating specialized investigative units focusing on financial investigations and asset tracing/freezing.

When managing a case, the sequencing of actions can be of the greatest importance. For instance, measures that pose a risk of disclosing to outsiders the existence of the investigation and, to some degree, its purpose (such as the interviewing of witnesses and the conducting of search and seizure operations), should not be undertaken until after other measures were taken, which will only be effective if the target has not been alerted. Besides, some procedures may become urgent if it appears that evidence could be destroyed or illicit proceeds be moved.[10]

Investigative teams may be assigned to specific target individuals, or focus exclusively on particular aspects of the case in complex investigations. For example, one group might be engaged in the tracing of proceeds, while others interview witnesses or maintain suspects' surveillance.

Table 1: Managing transnational or "Grand Corruption cases" [11]

Cases involving "grand corruption" or that have significant transnational aspects raise additional management issues. For example, cases where high level officials are suspected raise exceptional concerns about integrity and security and are likely to attract extensive media attention. Large-scale and sophisticated corruption is well resourced and well connected; making it more likely that conventional sources of information will either not have the necessary information or evidence or be afraid to cooperate. Senior officials may be in a position to interfere with investigations. The magnitude of proceeds in grand corruption cases makes it more likely that part of the overall case strategy is the tracing and forfeiture of the proceeds, and where they have been transferred abroad, obtaining their return. Allegations that senior officials are corrupt may also be extremely damaging in personal and political terms if they become public and later turn out to be unsubstantiated or false.

Transnational elements are more likely to arise in grand corruption cases. Senior officials realize that there is no domestic shelter for the proceeds while they are in office and generally transfer very large sums abroad, where they are invested or concealed. In many cases, the corruption itself has foreign elements, such as the bribery of officials by foreign companies seeking Government contracts or the avoidance of costly domestic legal standards in areas such as employment or environmental protection. The offenders themselves also often maintain foreign residences and flee there once an investigation becomes apparent.

Generally, transnational or multinational investigations require much the same coordination as do major domestic cases, but the coordination and management must be accomplished by various law enforcement agencies that report to sovereign Governments that have a potentially wide range of political and criminal justice agendas.

Coordination will usually involve liaison between officials at more senior levels and their foreign counterparts to set overall priorities and agendas, and more direct cooperation among investigators within the criteria set out for them. From a substantive standpoint, investigative teams in such cases will generally be much larger and will involve additional areas of specialization such as extradition, mutual legal assistance and international money laundering.

E. Choosing investigative methods and techniques

Determining which investigative tools to use depends on a variety of factors, including the nature of the alleged violations and the available resources.

In the course of the investigation, it is a normal progression to go from investigative measures that do not alert the targets that they are under investigation –research of public databases, collection of public information, informal interviews of potential witnesses that are not close connected with the targets, etc. - to measures that, once taken, allow the investigators to secure both evidences and proceeds of the crime. In other words, investigators must first arm themselves with as much information as possible to both insure that potential witnesses –and, where admissible, defendants- tells the truth, and also keep criminal proceeds from dissipating because the investigation becomes public.

The following paragraphs classify some of the investigative techniques used by several APEC economies in standard and complex or special investigative techniques. The following Chapters will specifically focus on the gathering of peripheral, digital and human evidence.

1. Standard investigative techniques

Interviewing witnesses and defendants

Conducting interviews is one of the techniques for investigators to gather evidence and information in furtherance of their financial investigation. Interviews with potential witnesses or suspects –for those member economies where cooperation of suspects might be exchanged by leniency- however, should not commence before considering the potential negative impact on the investigation by soliciting the witness's co-operation. Even if not required by the criminal procedure rules, detailed reports of investigation should be completed to document interview results. Interview reports may be helpful in refreshing investigators and witnesses' recollections of events during criminal or civil formal legal proceedings.

Still, the investigator should by no means be satisfied with interviews as a sole piece of evidence. Testimonies and facts recollected through informal interviews shall be tried to be re-confirmed through all other legal means of obtaining evidence to overcome the presumption of innocence.

Physical Surveillance

This is a useful technique to gain general background and intelligence and information on individuals/businesses, habits and relationships of suspects. It may also include electronic surveillance, through the use of visual surveillance in public places with the use of photography, video recording, optical and radio devices. Surveillance can be especially useful in financial investigations in cases involving the movement of bulk currency and by identifying “gatekeepers” involved in the development and implementation of ML schemes. Surveillance of targets can often identify where financial and related records might be stored and lead to the discovery of assets. In addition, surveillance can help corroborate financial data and identify other targets and associates.

Trash runs

Consists in searching the suspect’s discarded trash for evidence. It can be an effective way of obtaining leads where assets are maintained as well as help develop probable cause for more coercive measures and evidence for use at trial. Suspects frequently discard evidence, including financial records and correspondence that may be valuable to a financial investigation.

Searches and other compulsory measures to obtain evidence

These measures should be used to gather evidence of criminal activity that cannot be obtained by other means without authorization from a competent authority. The timely use of these powers to obtain evidence minimizes the opportunity for suspects to purge records and/or destroy evidence. In addition to seizing paper documentation, investigators should intercept or seize information from computers and other electronic devices, such as telephone, fax, e-mail, mail, public or private networks. The execution of these powers should always be properly planned and be lawfully conducted in accordance with existing policies and procedures.

2. Special investigative techniques

Although investigators of corruption cases tend to rely heavily on basic investigative techniques, good practice shows however that more focus should be given to the use of special investigative techniques, financial investigations and international cooperation for the successful investigation and prosecution of complex and cross border corruption crimes.

Special investigative techniques are applied by competent judicial, prosecuting and investigating authorities in the context of criminal investigations for the purpose of detecting and investigating complex criminality in order to gather information in such a way as not to alert the target persons.[12]

Special investigative techniques, although effective, entail serious risks that should be adequately addressed. Member economies should ensure: that their competent authorities are properly trained in using these techniques, that clear policy and procedural guidelines are established and followed, and that proper operational oversight is conducted at the managerial level.

The following techniques have proven useful in corruption and financial investigations:[13]

Intercepting communications

Electronic surveillance techniques, such as electronic intercepts of wire, oral communications, electronic media and the use of tracking devices, can be very useful in financial investigations. This technique can help identify co-conspirators, provide insight into the operations of the criminal organization, provide real time information/evidence that can be acted upon using other investigative techniques and can lead to the discovery of assets, financial records and other evidence. Competent authorities should be trained in these techniques in accordance with the basic principles of the domestic laws.

Controlled delivery

This is an effective investigative technique involving the transportation of contraband, currency, or monetary instruments to suspected violators under the control of law enforcement officers. Cross-border controlled deliveries can be performed in cooperation with customs and other foreign competent authorities, or on the basis of international agreements. Controlled deliveries are conducted to:

- Disrupt and dismantle criminal organizations engaged in smuggling contraband, currency, or monetary instruments across borders.
- Broaden the scope of an investigation, identify additional and higher level violators, and obtain further evidence.
- Establish evidentiary proof that the suspects were knowingly in possession of contraband or currency.

Identify the violator’s assets for consideration in asset forfeiture proceedings.

Cross-border observation

This investigative technique allows keeping a person who is located in a foreign economy under observation, with the authorization of the competent authorities of such economy. It may be used to keep under observation a person to which extradition may apply, or a third person who will probably lead to the offender.

Undercover operation

Undercover operations typically allow investigators access to key evidence that cannot be obtained through other means. An undercover operation is an investigative technique in which a law enforcement officer or a person cooperating with the competent authority, under the direction of a law enforcement authority, takes undercover action to gain evidence or information (e.g. by infiltration of an officer under false identity into a criminal group). This technique includes the use of undercover companies (*i.e.* the use of an enterprise or an organization created to disguise identity or affiliation of individuals, premises and vehicles of operative units), informants (*i.e.* voluntary confidential cooperation with individuals to obtain information about crimes being plotted or already committed; informants can operate openly or secretly, free of charge or for a fee, can be hired as permanent or non-permanent staff) and use of agents *provocateur* or integrity testing (*i.e.* an investigator or other agent acting undercover to entice or provoke another person to commit an illegal act).

Properly conducting undercover operations often requires substantial resources, extensive training and significant preparatory work. The resources it requires, the unique and diverse skill sets it demands and its inherent risks typically make this technique a last resort – normally after other investigative techniques have been unsuccessful. Various significant factors should be considered when envisaging an undercover operation, including the legal framework, whether positive results are actually likely to be achieved, and the reliability of the informants under use.

Given the inherent risk with this technique, undercover operations proposals should be *reviewed and authorized* by designated officials from the competent law enforcement authorities. These officials should be knowledgeable on all aspects of undercover operations. Moreover, the proposal should indicate that traditional investigative techniques have been utilized and have been largely unsuccessful and that the undercover operation is likely the only technique available to gather evidence of the suspected criminal activity. Only highly trained undercover agents should be used in undercover operations.

Undercover operations should be re-evaluated in an ongoing manner, and investigators should always be prepared for its termination. Termination criteria should be prepared in advance.

The actions performed by law enforcement during undercover operations should be in accordance with the basic principles of existing laws, policies and procedures, and all undercover officers should be highly trained before engaging in such operations.

CHAPTER II. BUILDING COORDINATION AND COOPERATION NETWORKS

The previous Chapter stresses the importance of ensuring adequate resources for an investigation and, among them, human resources. Selection of personnel, training and building trust exercises were pointed out as key pre-conditions for a successful team building strategy.

In all member economies, nonetheless, these human resources are usually distributed in an arrow of different State agencies and, sometimes, in the private sector. Therefore, rarely can anticorruption units build an internal team that satisfies all the required skill. More often, it is necessary to resort to counterparts in other agencies, such as tax agencies, customs, financial intelligence units (FIUs), supervisors of the banking, insurance and securities sectors, public procurement agencies, etc. Liaising with such agencies is usually subjected to both legal and practical challenges of coordination and cooperation.

This Chapter captures the best practices member economies have resorted to in order to overcome these challenges, in particular when liaising with FIUs at the domestic level (Section b) and with foreign counterparts of different nature (Section C).

A. Internal cooperation and coordination issues

The creation of institutional conditions that ensure that investigative specialized units can work closely with different competent authorities is fundamental for successful investigations. For example, information from tax authorities, oversight institutions, or FIUs can help tracing assets that may have been derived from corruption. Mechanisms that have been stressed for the promotion of intra and inter-agency cooperation include:[14]

- Establishing information sharing systems whereby all investigative services would be aware of previous or on-going investigations made on the same persons and/or legal entities so as to avoid replication.

- Establishing policies and procedures that promote the sharing of information/intelligence within intra-agency and inter-agency cooperative frameworks; such policies and procedures should promote the strategic sharing of the necessary information.

- Establishing a process whereby intra-agency or inter-agency disputes are resolved in the best interest of the investigation.

- Establishing written agreements such as Memorandums of Understanding (MoUs) between agencies to formalize these processes.

Given the need for autonomy and independence on the part of investigators, and taking into account the extreme sensitivity of many corruption cases, care must always be taken when establishing relationships between anti-corruption bodies and other government agencies (e.g. internal inspection and audit within government agencies), especially in environments where corruption is believed to be widespread.

Table 2: Multi-disciplinary groups or task forces

SOURCE: FATF Report. Operational Issues. Financial Investigations Guidance, June 2012, **p. 17-19**

Particularly in large and complex financial investigations, it is important to assemble a multidisciplinary group or task force to ensure the effective handling of the investigation, prosecution and eventual confiscation. There should be a strategic approach to intra-agency and inter-agency cooperation in an effort to support information/intelligence sharing within and between agencies and with foreign counterparts.

Multi-disciplinary groups or task forces serve to integrate information from different law enforcement and intelligence sources, which had previously been separated by organizational and technical boundaries. In some jurisdictions this requires changes in laws and regulations or may require formalized agreements such as Memorandums of Understanding (MoUs). These task forces leverage existing technologies and develop new technologies in order to provide cross-agency integration and analysis of various forms of data. Furthermore, this information is stored in centralized databases so that any future investigation of any new target of a participating task-force agency can be cross-referenced against that historical data.

Multi-disciplinary groups may comprise a range of individuals, including specialized financial investigators, experts in financial analysis, forensic accountants, forensic computer specialists, prosecutors, and asset managers. Experts may be appointed or seconded from other agencies, such as a regulatory authority, the FIU, a tax authority, an auditing agency, the office of an inspector general, or even drawn from the private sector on an as-needed basis. The multi-disciplinary groups should include individuals with the expertise necessary to analyze significant volumes of financial, banking, business and accounting documents, including wire transfers, financial statements and tax or customs records. They should also include investigators with experience in gathering business and financial intelligence, identifying complex illegal schemes, following the money trail and using such investigative techniques as undercover operations, intercepting communications, accessing computer systems, and controlled delivery. Multi-disciplinary groups should also consist of criminal investigators who have the necessary knowledge and experience in effectively using traditional investigative techniques. Prosecutors also require similar expertise and experience to effectively present the case in court.

B. Collaboration between law enforcement agencies and FIUs

Together with intelligence divisions of law enforcement and other competent authorities, Financial Intelligence Units (FIUs) are one of the competent authorities that can initiate or enhance financial investigations. Financial intelligence received by these agencies should be thoroughly analyzed and, expectedly, result in the proactive initiation of money laundering investigations.

The Egmont Group defines a FIU as a central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism; or (ii) required by national legislation or regulation, in order to counter money laundering and terrorism financing.[15]

A core function of FIUs is to analyze the information they collect and to disseminate the results of such analysis through competent enforcement authorities. FIU's analytical capabilities allow them to develop different intelligence products that can be useful to investigative authorities.

Member economies are free to establish their FIUs within the branch of the Government of their preference. In fact, around the world, there have been identified four institutional structures of FIUs:

- The judicial model of FIU is established within the judicial branch of government.
- The law enforcement model of FIU works in support of other law enforcement and judicial agencies. It may have concurrent or even competing investigative capacities over money laundering.
- The administrative model of FIU is a centralized, independent, administrative authority, which receives and processes information from the designated parties and transmits it, when deem appropriate, to law enforcement or judicial authorities for prosecution.
- Hybrid models of FIU combine elements of at least two of the previous FIU models.

A modern FIU can provide a range of services to anti-corruption and law enforcement agencies. These services range from simple data descriptions to complex analysis, including:

- scalable link analysis and spatial analysis of geographical locations and interactions
- text mining to find themes and concepts in unstructured data, and
- modeling to develop rules to explain and predict behavior.

Table 3: Best practices

Australia - 2010 "fusion project": Integration or 'fusion' of intelligence and investigative resources to develop the big picture of serious organised crime and corruption.

SOURCE: "The value of a multi-agency approach to detect, analyze and disrupt illicit financial flows", presentation by Mr. Adam Coin, Chargé d'Affaires, Australian Embassy, Santiago de Chile, at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

The purpose of fusion is to help Australian law enforcement agencies to see the bigger picture of organised and transnational crime. The bigger picture can't be seen if information and intelligence remains separated in multiple agencies. Fusion is the process of integrating and analysing those multiple sources. So far, the project has informed the design of various initiatives, including the Counter-Terrorism Control Centre and the Criminal Assets Confiscation Taskforce. Plans are also underway to establish the Australian Cyber Security Centre.

The Australian Crime Commission Fusion Centre brings together specialists from different government agencies, and different levels of government, with access to multiple information and intelligence holdings. The Fusion Centre includes staff from the Australian intelligence community, the Australian Crime Commission, the Australian Taxation Office, Australia's financial intelligence unit (AUSTRAC), the national welfare agency (Centrelink), the Department of Immigration and Citizenship, and law enforcement agencies. Staff from these diverse agencies bring expertise in financial investigation, operational psychology, data-mining, statistical analysis, database management and architecture. They put the pieces together from different agencies to produce a more comprehensive picture of criminal targets, risks, threats and vulnerabilities.

Although only established in 2010, the benefits of the project are already apparent. For example, in early 2013, fusion intelligence detected a series of suspicious international transactions from Australia valued in excess of $A20 million. Intelligence also showed the use of false identities and credit cards. Following this detection, Australian law enforcement agencies located two significant methyl amphetamine laboratories.

Fusion has also paid dividends for the detection of international money laundering and the recovery of assets. For example, in late 2012, fusion identified likely proceeds of crime in excess of $38 million being transferred to a foreign jurisdiction. In another investigation, significant money laundering involving profession facilitators was identified. These detections are now being investigated.

1. Accessibility of FIU disclosures in financial investigations

Financial disclosures and FIU analysis are a valuable source of information. AML/CFT disclosures of reporting entities, whether suspicious transaction reports (STRs) or systematic information required by AML/CFT legislation, can help investigators connect other pieces of information, provide information on where the proceeds of criminal activity are located and when and where these funds are moved.

Effective financial investigations are thus characterized by extensive law enforcement use of FIU information and exchanges of information and personnel. Investigative authorities should be able to ask the FIU for relevant information they may hold when conducting lawful investigations and FIUs should be able to respond to information requests from competent authorities.[16]

Requesting all relevant FIU information should be a basic step in a financial investigation. This should be included as part of a routine investigator "checklist." Therefore, it is essential that investigators have timely access to financial disclosures filed in their jurisdictions. This access does not have to be direct but should be prompt so as to facilitate the incorporation of significant and relevant findings and to further active investigations. Some member economies provide their investigative authorities with direct –although restricted– access to the FIU's database, being able to directly query such database under certain circumstances. Arrangements for investigators' access to the FIU's database should take into consideration information handling issues such as confidentiality, privacy and data protection as well as the respect for international human rights individual rights.

Finally, the FIU will hold, or have access to its own information and information gathered from third parties (both domestic and foreign) that can enhance investigations if provided at the request of the investigative authorities. FIUs responses to specific requests can support existing activity by identifying and locating proceeds of crime and supply information, which can assist in securing convictions and confiscations. Some of this information will be confidential or sensitive, and the manner in which it can be shared may be restricted. Restrictions may be imposed by law or by the third party originator of the information. Thus, when receiving information from the FIU, investigators should note the existing restrictions on its use. It is important that law enforcement personnel handling this information be trained and knowledgeable on the applicable disclosure rules.[17]

2. Proactive sharing of information between the FIU and investigating authorities

Both the FIU and the investigative authorities should seek to work together as a team, sharing information in appropriate circumstances to support financial investigations. Providing an FIU with an information requirement –detailing information priorities– can assist the FIU in identifying useful information for spontaneous dissemination. Many investigative authorities have seconded personnel working in the FIU, or FIU personnel seconded to investigative authorities in order to facilitate co-operation and information exchange. Single points of contact in investigative authorities and the FIU can also assist consistent, efficient information exchange.

Documenting how competent authorities and FIUs interact and establishing communication channels can provide clarity on the procedures and processes that are required in order to exchange information appropriately. Formal arrangements between investigative authorities and the FIU can be documented in MoUs, memorandum of agreements (MoAs) and standard operating procedures (SOPs). Agreeing on the use of standard electronic reports and request forms that can be securely exchanged between the FIU and investigative authorities can also facilitate efficient exchange of information. When exchanging bulk or structured data in relation to financial investigations (such as computer files with analysis results) consideration should also be given to the compatibility of the software used by competent authorities and the FIU.

Regarding STRs in particular, it should be noted that a financial investigator's understanding is often greatly increased when STRs or disclosure related information is compared with information from other sources (including existing intelligence on illegal activities, criminal records, ongoing investigations, historical investigative reports, and in some cases income tax records). It is therefore essential that law enforcement and the FIU work together to identify those STRs that merit further investigation and ensure that both parties understand what checks have been conducted and which aspects of the disclosure are the most useful to pursue.

The need for efficient utilization of limited resources is a challenge faced by most investigators. When necessary, STRs should be prioritized on the basis of their relative significance, as well as the general investigative priorities and strategies of the economy. Where a large number of STRs are generated each month, software that works on the basis of pre-established criteria is usually needed to narrow the field of STRs. After such a basic filter, experienced and sufficiently trained support personnel can be designated to continue the prioritization exercise.

3. Use of FIU's intelligence as evidence

Financial disclosures and FIU analysis are usually considered a particular category of information. As stated, they constitute a particularly valuable source of information to law enforcement and, particularly, financial investigators. Given that the main focus is on the use of STRs, the unique nature of this data should be highlighted.

In most member economies, STR information is used for intelligence purposes and is not directly used as evidence in court proceedings. Intelligence information obtained through FIUs shall usually need to be re-obtained through Court proceedings, whether domestically or through mutual legal assistance requests, when the information has been obtained from a foreign FIU. The rationale behind this principle is that the restrictions of individual rights –sometimes privacy, sometimes property-, which might follow the introduction of such information into a legal proceeding is subject to Court authorization.

In addition, and for the same reasons, there are also strict confidentially rules associated with access to and use of this information. It is essential that only competent and appropriately trained law enforcement officers have access to this information.

4. Ensuring the proper use of financial intelligence analysis and data

Information sharing and feedback among the FIU, other domestic partners and international counterparts must be subject to strict safeguards –as set out in law or cooperation agreements– to ensure proper use of the data.

It is important to determine how intelligence can be made available to operational authorities and developed into investigative leads or evidence. In order to promote the timely sharing of information, especially at the international level, FIUs can provide guidance on information handling and, where possible, prior consent to its sharing. Such arrangements are usually discussed bilaterally between FIUs in order to address privacy concerns and to ensure that the information is shared lawfully and appropriately with the competent authorities conducting a financial investigation. If prior consent (also known as third party rule) is required, FIUs should establish mechanisms whereby such consent is obtained in a timely manner.

Because of the practical differences among jurisdictions, there is no exact model for STR utilization that would necessarily fit every member economy. Regardless, member economies should consider putting into place mechanisms that allow their investigative authorities prompt delivery of FIU information and analysis in furtherance of their investigations. The procedures for delivery should be clearly delineated and subject to strict safeguards to ensure proper security and use of the information. Any model should have in place monitoring systems while ensuring that the process is free of unnecessary hurdles.

C. International cooperation with investigative purposes

International cooperation is highly important for successful investigations and, in particular, for financial investigations. Financial investigations often reach beyond domestic borders and gathering of evidence abroad is a key element in many corruption and money laundering investigations. In complex cases involving many jurisdictions, where information possessed by one of the economies is usually not enough to show an illegal scheme, contacts with law enforcement authorities of other economies involved and the proactive exchange of information are a key factor of success in investigating and prosecuting a case. In investigations ending with asset repatriation, international cooperation will also be fundamental. The combination of informal cooperation among law enforcement authorities and formal international cooperation mechanisms has led to many successful corruption investigations worldwide.

It is thus important that competent authorities from all member economies immediately focus on both formal and informal international cooperation efforts throughout the case, ensuring they can rapidly, constructively and effectively provide the widest range of international co-operation in relation to corruption offences.

International cooperation can be informal or formal. Informal cooperation is usually referred as the mechanisms for obtaining intelligence with investigative purposes; formal channels of international cooperation refer to the procurement of information with evidentiary purposes. Formal mutual legal assistance will always be necessary when the requested assistance either involves coercive measures –e.g., compulsory summoned witnesses- or the restriction of individual rights –e.g., restraining or confiscation measures-, which will normally require Court authorization.

While formal cooperation is channeled through Mutual Legal Assistance requests or other formal requests to foreign countries through a designated central authority, typical informal channels used by financial investigators include:

- Contact existing liaison officers or investigators in or of the foreign jurisdiction.
- Exchange information between national (or regional) police units using channels such as INTERPOL and other regional law enforcement bodies.
- Inform the national FIU which has a possibility to contact its foreign counterparts and collect further intelligence through the Egmont Secure Web or by other means.

The remaining of this section describes the main channels for informal international cooperation as well as the most salient requisites of mutual legal assistance requests.

1. Informal cooperation networks

The establishment of informal contact between officers and investigators of member economies should be the first step towards effective cooperation. Whenever possible, information or intelligence should initially be sought through police-to-police contact, which is faster, cheaper and more flexible than the formal route of mutual legal assistance. Such contact can be carried out through local liaison officers, under any applicable memoranda of understanding, through Interpol, or through any regional arrangements that are available.

Through such informal assistance investigators can gather information more quickly, build the necessary substantive foundation for an eventual formal request, and develop a strategy that best accords with the advantages and limitations of the legal systems of the involved jurisdictions. Both the United Nations Convention against Corruption (UNCAC)[18] and the FATF Recommendations[19] highlight the importance of the availability of informal cooperation and assistance mechanisms among counterpart agencies.

Economies should ensure that domestic laws authorize direct contact between domestic authorities—including law enforcement agencies, financial intelligence units, and prosecutorial agencies—and their foreign counterparts. Authorities in requested jurisdictions should be permitted to provide some information and informal assistance to their foreign counterparts without requiring a formal MLA request.

Most member economies are in the position to provide the following types of informal assistance without a written formal request:

- public records, such as land registry documents, company documents, information about directors and shareholders, and filed company accounts;
- potential witnesses to determine if he/she is willing to cooperate voluntarily and take statements from voluntary witnesses, provided that contact with witnesses is permitted under such circumstances;
- provide basic subscriber details from communication and service providers that do not require a court order.[20]

Table 4: Best practices

Best practices to help strengthen legal frameworks and ensure that asset tracing and financial investigations can be conducted effectively include having appropriate procedures and the legal framework to allow the informal exchange of information, the use of appropriate regional and international bodies to facilitate cooperation, the spontaneous sharing of information with proper safeguards and the entering into asset sharing agreements.[21]

- Police-to-police communication

Police-to-police communication can be a very useful way for the APEC economies to acquire information, especially in the early phases of an investigation that may later on require a formal MLA request.[22] Matters such as locating witnesses or suspects, conducting interviews, sharing police files or documentation on a person or assessing whether a witness would be prepared to speak with investigators can all be done through police agencies, with no need to resort to a mutual legal assistance request. Police agencies have well-established networks of *liaison* officers throughout the world, and lines of communication and protocols with the police agencies that they consistently deal with. INTERPOL is the most developed worldwide police network.[23]

- Agency-to-agency communication

An example of agency-to-agency communication is the one between the central authorities, investigatory authorities as well as the liaisons that report to them. These lines of communication complement the lines that the police and INTERPOL have already established.

- Consular communications

Some APEC economies rely on their consulates abroad to assist in obtaining information in financial investigations and as a conduct for obtaining help to prepare a formal MLA request. Mexico, for instance, uses its consulates to obtain evidence, declarations or information regarding particular investigations or judicial cases.[24]

a. Personal networking

Personal contacts between members of competent authorities, prosecutors and investigators from the requesting and requested economies (through a telephone call, an e-mail, a videoconference or a face-to-face meeting) and developing working level cooperation are of great importance in order to achieve open communication channels and develop the familiarity and trust necessary to achieve the best results in mutual legal assistance casework.

Relevant information may be obtained more quickly and with fewer formalities through direct contact with counterpart law enforcement agencies and FIUs or from law enforcement attachés. Such contact can be initiated through existing police attaché networks, or between prosecutors' staff of central authorities, through the United Nations International Drug Control Programme (UNDCP) list of competent authorities, or through less formal structures such as the International Association of Prosecutors or simply personal bonds. This kind of assistance may lead to a more rapid identification of evidence and assets, confirm the assistance needed and even more importantly provide the proper foundation for a formal MLA request.

Establishing early contact with foreign counterparts aids investigators in understanding and foreseeing how to address the potential challenges that might emerge from a different legal system, in obtaining additional leads and in forming a common strategy. It also gives the foreign jurisdiction the opportunity to prepare for its role in providing cooperation.

In order to constructively and effectively provide the widest range of international cooperation, it is essential for financial investigators to discuss issues and strategy with foreign counterparts. Such discussions should involve consideration of conducting a joint investigation[25] or providing information to the foreign authorities so that they can conduct their own investigation.

If the financial investigation is in an early stage or if concerns about the integrity or independence of potential counterparts are at stake, discussion from a "hypothetical" perspective is recommended. Such discussions allow all involved parties to get a better understanding of the parameters and requirements of an investigation without having to discuss too many specific details, which can be shared at a later stage if necessary.

Finally, it is important for investigators and prosecutors who are daily involved in corruption cases to regularly attend training events and seminars at the regional or international level.

b. The International Criminal Police Organization (Interpol)

Interpol is the world's largest international police organization, with 190 member countries.[26] It was created in 1923 to facilitate cross-border police co-operation, and support and assistance to all organizations, authorities and services whose mission is to prevent or combat international crime (even where diplomatic relations do not exist between particular jurisdictions). Its four core functions are: (i) to maintain a secure global police communication service; (ii) to provide police with operational data services and databases; (iii) to offer operational police support services; (iv) training and development[27].

c. The Egmont Group

Informal contact with the FIU of another member economy for information purposes can be achieved through direct contact between the implicated agencies or through the Egmont Group, when both members belong to such forum.[28]

The Egmont Group, created in 1995, provides a forum for FIUs around the world to enhance support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes. This support includes:

- expanding and systematizing international cooperation in the reciprocal exchange of financial intelligence information,
- increasing the effectiveness of FIUs by offering training and personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs,
- fostering better and secure communication among FIUs through the application of technology, presently via the Egmont Secure Web (ESW), and
- promoting the establishment of FIUs in those jurisdictions without a national anti-money laundering/terrorist financing program in place, or in areas with a program in the beginning stages of development.

The Egmont Group has now over 130 members.[29]

A secure encrypted capability designed to share information over the Internet; Egmont's Secure Web facilitates communication among group members via a secure e-mail, also allowing them to access meeting minutes and related documents, as well as a variety of published materials of the Egmont Group.

2. Formal cooperation

Formal cooperation is often the only way in which evidence can be obtained from another jurisdiction to be presented in the court. Formal types of assistance include: letters rogatory, letters of request, Mutual Legal Assistance requests and requests under bilateral or multilateral treaties. In order to legally obtain evidence that is admissible in court, investigators and/or prosecuting authorities must make use of the applicable international arrangements which may be based on reciprocity, MoUs, bilateral or multilateral agreements. Once a decision has been made as to which jurisdictions have responsibility for prosecuting and/or investigating different sides of a given case, mechanisms should be agreed in order to ensure that all relevant evidence can be made available in the competent jurisdiction in a form that will allow production in a criminal court respecting the due process of law.

Table 5: The Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand. It consists of 41 members and a number of international and regional observers. Some of the key international organizations that participate with, and support the efforts of the APG in the region include the Financial Action Task Force, the International Monetary Fund, the World Bank, the OECD, the United Nations Office on Drugs and Crime, the Asian Development Bank and the Egmont Group of Financial Intelligence Units.

The purpose of the APG is to ensure the adoption, implementation and enforcement of internationally accepted anti-money laundering and counter-terrorist financing standards as set out in the FATF Forty Recommendations and FATF Eight Special Recommendations.

The effort includes assisting countries and territories of the region in enacting laws to deal with the proceeds of crime, mutual legal assistance, confiscation, forfeiture and extradition; providing guidance in setting up systems for reporting and investigating suspicious transactions, and helping in the establishment of financial intelligence units.

Chapter III: The Gathering of Information and Evidence

Prosecuting and proving a crime is often much more difficult than investigating and solving it. Due to the dire consequences of a criminal conviction for the fundamental rights of the convicted person, criminal cases have a stricter burden of proof than civil cases. In order to overcome the presumption of innocence and for a person to be convicted, that person must be proved guilty, either with certainty or –depending on the economy's legal system- "beyond any reasonable doubt".

Therefore, the gathering of credible information and evidence that supports the commission of a crime is often essential in the early stage of an investigation, since it allows law enforcement agencies to move forward by securing warrants for search, seizure, or intercepting phone calls and e-mails.

In order to be Court admissible, evidence must be obtained in accordance with the applicable criminal procedure laws as well as the constitutional rights of the defendants or any other affected third party. Due the fact that unlawfully obtained evidence could be declared inadmissible in court and therefore jeopardize the success of the prosecution or confiscation, all evidence should be legally obtained and, to that purpose, law enforcement agencies should be well aware of the legal framework applicable to the evidence collection process. Legal experts' advice should always be sought by agencies in dealing with the gathering of evidence.

Once evidence has been legally collected, it should be subject to an assessment in order to review the progress of the investigation and explore whether any additional line of enquiry can be identified.[30] Investigators are advised to follow a standard model of evaluation –like the one shown in the following flow figure– since it will allow them to evaluate the collected material in a consistent, structured, and auditable way.[31]

1 Setting the objective of the evaluation

In the early stages of an investigation, the objectives are likely to be broad and concerned with whether a crime has been committed, whether a suspect and witnesses can be identified, what material can be gathered, etc.

As the investigation progresses and initial ends are achieved, the objectives will narrow. They will vary depending on the crime, the available material and the stage of the investigation. The evaluation process should be sufficiently flexible to accommodate such changes.

2 Evidential filters

Relevance

Whether gathered materials have some bearing on any offence or person under investigation, or on the surrounding circumstances of the case, must be evaluated

Reliability

The reliability of materials should be reviewed during the evaluation process to ensure that any potential problems have not been overlooked. Investigators should have a clear understanding of the impact the reliability of material may have on the investigation and the strength of the prosecution case. An element can have high reliability if it can be corroborated by an independent source, and less reliability if it cannot be corroborated and conflicts itself with other materials gathered in the investigation.

Admissibility

This test should ensure the investigators that the gathered materials will be available to the courts in an evidentially acceptable format. Investigators must be aware of the legal framework and must seek legal advice on what constitutes an acceptable evidential format in relation to any material.

3 Organizing knowledge

In the first instance the objective of an investigation is likely to be broad and concerned with establishing what information there is, what type of incident is being investigated, whether or not a crime has been committed and if there is a suspect. The 5WH formula (Who – What – When – Where – Why – How) has been found to be a highly effective way for investigators to organize their knowledge in the early stages of an investigation (See Chapter IV, Section B.3 for further development of this formula regarding profiling).

Who are the victim(s), witnesses, and suspect(s)?
Where did the offence take place?
What has occurred?
When did the offence and other significant events take place?
Why was this offence committed?
How was the offence committed? Assess the use of skills or knowledge used by the offender.

Subsequent evaluations will replace the broad objectives with more specific objectives. The way in which investigators then choose to organize their knowledge will change to match these more specific objectives.

4 Testing Interpretation

There are a number of ways in which investigators can test the validity of their interpretations of the gathered material.

Self-review: Investigators should thoroughly check their work and review any assumptions they have made during the evaluation process.

Peer review: Checks by supervisors or colleagues provide a second opinion on the interpretation of material.

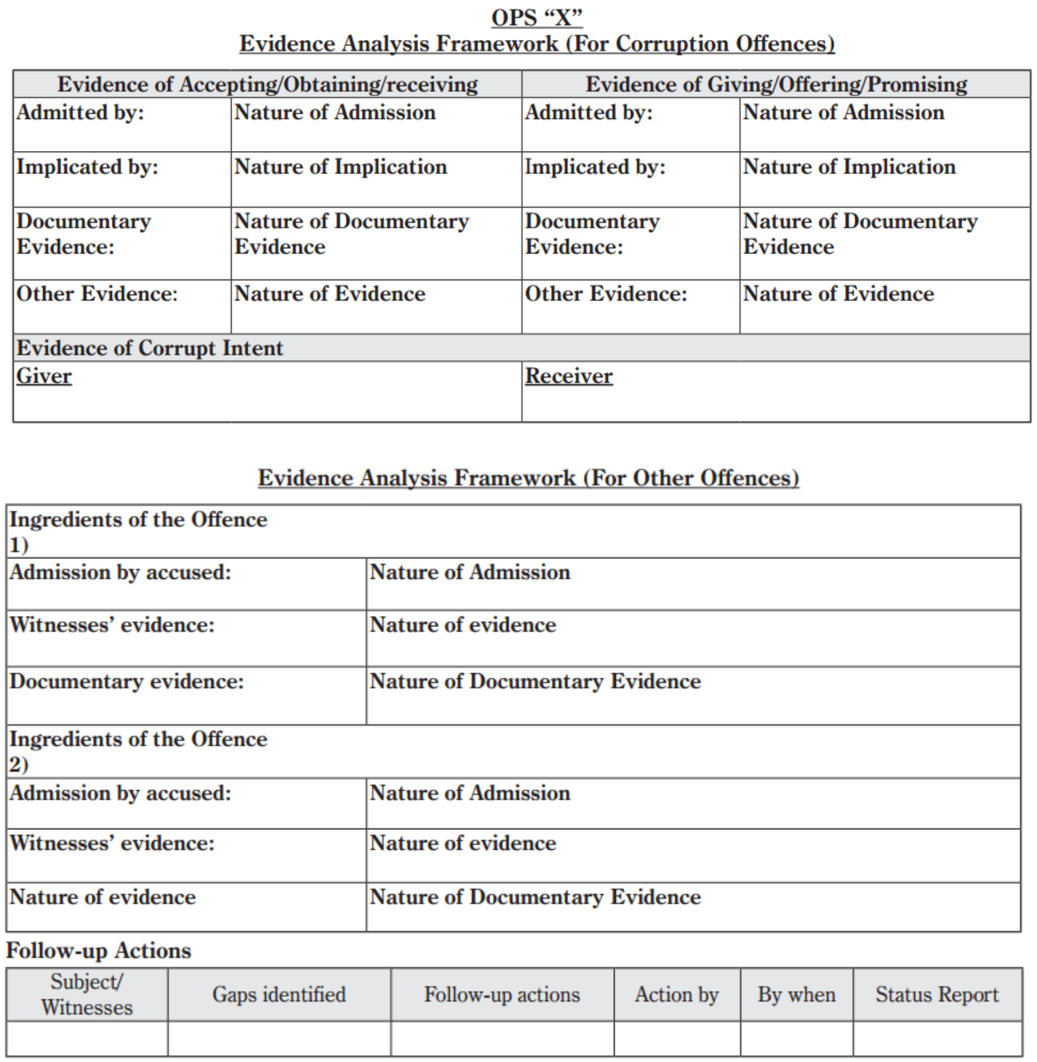
Expert review: Where investigators use material produced by experts such as forensic scientists, they should consult the expert to ensure that the outcome of the evaluation is consistent.

Formal review: In complex cases a formal review of the investigation can be carried out by a suitably qualified officer.

Table 6: Best Practices - Evidence gathering.

SOURCE: KOH TECK HIN, Investigation and Prosecution of Corruption Offences, (Singapore), Resource Material No. 86, Visiting Experts' Papers, 14th UNAFEI UNCAC Training Program, Tokyo, March 2012, pp. 104 ff.; CORRUPT PRACTICES INVESTIGATION BUREAU (CPIB), elaboration dated Dec 2013.

When we make use of the four competencies of intelligence, interview, forensics and field operations, we also focus on collecting and consolidating the evidence. From the evidence, we review the case. Sometimes, we sit together and discuss in case conferences to go through these issues - Do we have the evidence to charge anyone? What evidence is there when we proceed to charge? We make use of an evidence matrix (see table attached below).



OPS "X"

Evidence Analysis Framework (For Corruption Offences)

Evidence of Accepting/Obtaining/receiving		Evidence of Giving/Offering/Promising	
Admitted by:	Nature of Admission	Admitted by:	Nature of Admission
Implicated by:	Nature of Implication	Implicated by:	Nature of Implication
Documentary Evidence:	Nature of Documentary Evidence	Documentary Evidence:	Nature of Documentary Evidence
Other Evidence:	Nature of Evidence	Other Evidence:	Nature of Evidence
Evidence of Corrupt Intent			
Giver		Receiver	

Evidence Analysis Framework (For Other Offences)

Ingredients of the Offence 1)	
Admission by accused:	Nature of Admission
Witnesses' evidence:	Nature of evidence
Documentary evidence:	Nature of Documentary Evidence
Ingredients of the Offence 2)	
Admission by accused:	Nature of Admission
Witnesses' evidence:	Nature of evidence
Nature of evidence	Nature of Documentary Evidence

Follow-up Actions

Subject/ Witnesses	Gaps identified	Follow-up actions	Action by	By when	Status Report

This matrix has facilitated our case review and decision making process. Evidence of accepting/receiving/ obtaining gratifications is reflected in the table, where officers document *actus reas*, inputting details of the corrupt transactions which the subject has admitted to in his statements, e.g. when did the transaction occur, who did he hand the gratification over to, what are the documentary evidence, etc. Next to the information, is the detailing of documentary or other evidence of giving/offering/promising of the corrupt transactions. Usually for easier reference, the evidence for giver and receiver involved in the same transaction are placed next to each other, quoting the exact paragraph of the subject's statements where the information was extracted from. As for the evidence on corrupt intent, it is also recorded in the table, and it includes details such as what are the gratifications meant for.

In addition, we also need to address the legal aspects. We understand that in some countries, the anti-corruption agency has their in-house legal experts and some agencies also conduct prosecution themselves In the Singapore system, the Corrupt Practices Investigation Bureau (CPIB) does not have in-house legal experts but is part of the criminal justice system which comprises the Attorney-General's Chambers (AGC), the Courts and other law enforcement agencies. The Courts represent the adjudicating arm; the AGC serves as the prosecuting arm, while CPIB and other law enforcement agencies form the investigative arm. CPIB is the only agency authorized to investigate into corruption offences. For all corruption cases, when investigation is concluded, the Public Prosecutor's consent must be obtained before prosecution against the corrupt offender can proceed. Thereafter, the accused will be brought before the court which will determine if the offender is guilty of the offence(s). In sum, after CPIB completes our investigation, we will submit our findings (including recommendations of corresponding charges to the AGC) for their consideration. AGC's decision on whether to proceed with prosecution is final. There is thus an inherent check and balance mechanism in our criminal justice system where the powers to investigate and prosecute corruption offences are separate and do not reside with any one agency.

In terms of prosecution, as we are prepared to prosecute both the givers and receivers of bribes, we have to stage our prosecution of the accused persons in sequential order. Sometimes the receiver is prosecuted first and the giver is the prosecution witness. After the case is over, the giver is prosecuted and the receiver in turn becomes the witness. This can present some challenge especially when there is not much independent evidence apart from what the giver and receiver say about the crime. Therefore, as we adopt this tough stance against both sides of the corruption crime, it is the responsibility of CPIB to ensure that it gathers strong evidence on the case so as to be able to prosecute all parties involved. So far, our conviction rate is of above 95% each year and this bears testimony to the strength of cases brought to the Court.

There are instances where the only evidence we have is from the giver and the giver is not willing to testify unless he is given immunity from prosecution. As a rule, the Attorney General's Chambers does not grant immunity easily. It will be under exceptional grounds if immunity is granted.

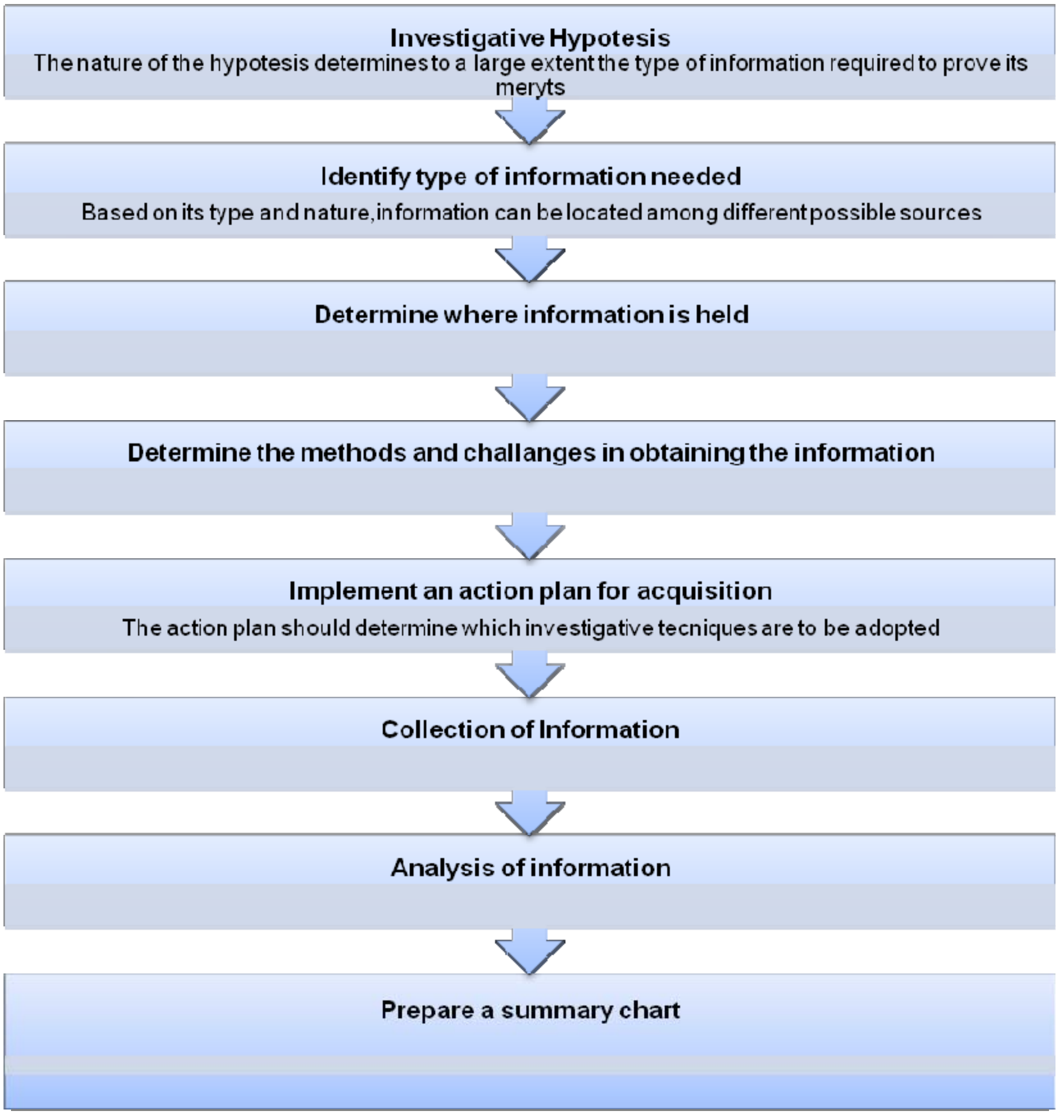
There may be cases in the public sector, where after investigation, there is no evidence of corruption but there is evidence that the public official had infringed some government rule or regulation. In such situations, CPIB will provide the information to the Public Service Commission or to the officer's Department or Ministry for them to take departmental disciplinary proceedings against the said officer.

In some cases, besides dealing with the culprits, after the case is over, CPIB may identify flaws or loopholes in the system, work processes or procedures of the affected government departments and offer some recommendations or suggestions for them to consider as they work towards mending the flaws and loopholes.

A. Sources of information

A variety of sources can be relevant to financial investigations, including interviews, searches, forensic examination of computer(s), collection and analysis of financial and business records, tax authorities' reports, etc.[32]

The process illustrated in the following flow chart synthesizes a recognized international best practice to be follow all along the process of gathering of information and evidence.


Investigative Hypotesis
The nature of the hypotesis determines to a large extent the type of information required to prove its meryts
Identify type of information needed
Based on its type and nature, information can be located among different possible sources
Determine where information is held
Determine the methods and challanges in obtaining the information
Implement an action plan for acquisition
The action plan should determine which investigative tecniques are to be adopted
Collection of Information
Analysis of information
Prepare a summary chart

There will be differences within each economy in the way that various types of information can be made available to investigative authorities and this may be influenced by legal requirements. The producers and owners of the relevant pieces information and intelligence products will also differ between economies[33].

There are several ways to categorize potential data sources. The Inter American Drug Abuse Control Commission of the OAS (CICAD) has proposed a classification of sources of information that is also applicable to corruption investigations:[34]

Patrimonial

Sources of information related to asset ownership of an individual or company (vehicles, real estate, horses, jewels, industrial real estate, airplanes, stocks, weapons, etc.)

Personal

Sources of information related to data of an individual such as marriage status, contact information, phone number, passport number, occupation, etc.

Legal

Sources of information related to civil, criminal, business, and labor litigation of an individual or company.

Business

Sources of information related to economic activity or business conducted by an individual or company.

Police

Sources of information related to traffic infractions, fines, or any other relevant police information.

Corporate

Sources of information related to incorporation of companies and change in partnership quota, trust funds, board of directors, etc.

Normative

Sources of information related to a country's norms and regulations, and its jurisprudence.

Another useful way to categorize information is according to the nature of the source where it can be retrieved:

Criminal records and intelligence

Law enforcement information related to the subjects under investigation. Information such as previous arrests, indictments, convictions, but also reports of links with known criminals. Criminal information is typically gathered from surveillance, informants, interviews/interrogation and data research, or may be just picked up “on the street” by individual police officers.

Local Force Intelligence System

Information, including bank account details and telephone numbers, may be held on local databases.

AML/CFT Disclosures

In addition to suspicious transaction reports (STRs), this includes other information as required by national legislation such as cash transaction reports, wire transfer reports and other threshold- based declarations or disclosures.

Financial Information

Information about the financial affairs of entities of interest that helps to understand their nature, resources, structure and capabilities, and it also helps predict future activity and locate assets. This goes beyond the information contained in AML/CFT disclosures and is normally maintained by private parties, including bank accounts, financial accounts, other records of personal or business financial transactions and information collected in the context of meeting customer due diligence (CDD) obligations.

Examples:[35]

Financial Institutions

Information held by financial institutions can show the lifestyle of a person and whether they are living beyond their means. These can inform an investigator of payments to and from other persons, the lifestyle of the individual (their wealth, the turnover in their account), their spend patterns (for example, where they went on holiday, their travel, meals, hobbies and other interests), and any financial problems.

Commercial Service Providers

Merchant service providers, such as mobile phone companies, utility companies or firms that deal with merchants’ claims for reimbursement for credit or debit card payments by customers, hold a variety of information of potential use to an investigation. This can include a person’s location at a certain time or details of any electronic payments. Investigators can apply for production orders to obtain information from the financial institution that administers the chip and PIN or swipe systems (such as Link), which can then be followed up.

Credit reference databases

Credit reference agencies provide data access systems that can be used in criminal investigations allowing authorized officers to obtain information on an individual’s financial relationships and status. This information can assist in the prevention or detection of crime and apprehension and prosecution of offenders, or the assessment or collection of any tax or duty.

Classified information

Information that is gathered and maintained for national security purposes to include terrorism financing information. Access is typically restricted by law or regulation to particular groups of persons.

Open Sources

All information that is available through open sources such as the internet, social media, print and electronic media, as well as via registries operated publicly or privately.

Regulatory information

Information that is maintained by regulatory agencies; access is typically restricted to official use only. This category of information could be held by central banks, tax authorities, other revenue collecting agencies, registry agencies, etc.

Table 7: Warning – Do not leave footprints

SOURCE: Association of Chief Police Officers (ACPO), *Practice Advice On Financial Investigation,* 2006, p. 20.

There are various open and closed sources where financial information can be obtained. The enquiries made to obtain this information can, however, leave their own footprints. If an FI makes an enquiry with a Money Laundering Reporting Officer (MLRO) at a financial institution, the institution will make a note of the enquiry, including its purpose. The investigation being conducted may involve the use of covert investigation techniques. As such financial enquiries could result in those investigations being compromised. Prior to making the relevant financial enquiry, consideration must be given to the type of investigation being undertaken. As such any enquiries should be progressed in consultation with the FIU.

B. Gathering peripheral evidence

At the preliminary stage of any investigation, law enforcement agencies should rapidly gather information from all available sources. Data collected in this phase can therefore provide the factual basis to bring the investigation to the next stage, which might involve the need for a judicial warrant to be applied for before the competent authority. Because the data collected might be filed in a judicial proceeding, the acquisition process is a sensitive moment.

At this stage, immediately available sources are in particular the so-called “open sources” and government agencies databases (publicly and not-publicly available).

Those are typically referred to as the source of first resort, because every information collector should exploit them as the first step in the information-collection process.

1. Open Sources

a. General Aspects

Open source information has been defined as «publicly available information that anyone can lawfully obtain by request, purchase, or observation».[36] The use of open sources techniques is a rising area of intelligence gathering. As the public globally embraced the World Wide Web in the mid-to-late 1990s, the internet emerged as the primary source for search for all types of information. In the so-called "information age", the Internet provides access to a huge amount of significant, updated information, which has proven to be of dramatic importance for law enforcement agencies. In other words, almost everything is online: in 2008, for example, Google had indexed 1 trillion of addresses, which constitutes just a small part of the Internet.[37]

Originally developed for security purposes, the internet became widely used for academic and commercial research in the 1980s. In the late '90s, the U.S. GAO had already noted that investigators would have found significant advantages on accessing sources online rather than using any other information medium, and that «the internet provides enormous resource potential for investigators in a timely and cost effective manner and is often more up-to-date than its paper counterparts.»[38]

Internet-based services using Web 2.0 technology have become increasingly popular. Web 2.0 technologies are a second generation of the World Wide Web as an enabling platform for web-based communities of interest, collaboration, and interactive services. These technologies include web logs (known as "blogs"), "wikis," which allow individual users to directly collaborate on the content of Web pages; "podcasting," which allows users to publish and download audio content; and "mashups," which are web sites that combine content from multiple sources. Web 2.0 technologies also include social media services, which allow individuals or groups of individuals to create, organize, edit, comment on, and share content. These include social networking sites (such as Facebook and Twitter) and video-sharing web sites (such as YouTube).[39]

As reported by the U.S. Government Accountability Office in 2011, social media-related sites have become the most visited websites in the web.[40] Of course, quantity of information does not equal quality of information. Investigators must ensure that the information collected from open sources is accurate and reliable. The challenge, particularly when massive amounts of information are available, is to make good end-user decisions about what information should be kept and which information should be discarded.[41]

Open source information has often held a second-class status in the intelligence world because of the erroneous assumption that people, movements, and conditions that pose threats would not have information available about their intent, characteristics, or behavior in the open.[42] However, information can be made publicly available for many reasons: because the person needs so or the applicable laws require so, due to the individual's carelessness, and so on.

Open sources can be used for a variety of purposes. One of the most common uses is to identify and verify a wide range of facts: personal identity information, addresses and phone numbers, e-mail addresses, vehicles known to have been used, property records, are among a wide variety of other facts that can easily be identified through open source public and commercial databases and directories.[43] This type of tool can also be used as a mean to identify criminal offenders. Indeed, it has been remarked that in a surprising number of cases people made incriminating statements in open sources. While those statements alone will not meet the burden of proof for conviction, they clearly establish a criminal predicate and basis for further inquiry.[44] Finally, open sources can help in understanding the motivation or rationale of individuals involved in criminal behavior.

Today, the significance of open sources techniques has been widely recognized, and they have proven to be especially useful in corruption and money laundering investigation, as well as in the process of recovering stolen assets.[45] Its importance has also been remarked by the US 9/11Commission, which recommended to add a new Open Source Agency to the U.S. intelligence structure.[46] For these reasons, law enforcement agencies should rely upon open sources techniques more often, which should be incorporated in the agencies' intelligence plan.

Open sources intelligence includes methods of finding, selecting and acquiring from publicly available sources, and analyzing such information to produce credible intelligence. Open source is distinguished from research in that it applies the process of intelligence to turning hard data and information into intelligence to support strategic and operational decisions.[47]

Open source information is wide-ranging. Examples of categories of open source information include:[48]

All types of media

Example: www.newslink.org

Shortwave broadcasts and conversations

Examples: www.shortwave.be, www.blackcatsystems.com/radio/shortwave.html.

Publicly available databases

Examples: www.searchsystems.net, www.factfind.com/database.htm

Social networking sites and web-based communities

Examples: www.facebook.com, www.twitter.com, www.myspace.com

Directories

Example: www.mypeoplesearch.com (only US and Canada users allowed)

Databases of people, places, and events

Examples: www.namebase.org, www.searchsystems.net, www.blackbookonline.info

Open discussions, whether in forums, classes, presentations, online discussions on blogs, or general conversations

Wikis

Example: www.wikipedia.com

Government reports and documents

Scientific research and reports

Example: www.fas.org

Statistical databases

Example: www.bjs.gov

Commercial vendors of information

Example: www.acculeads.com

Web sites that are open to the general public even if there is an access fee or a registration requirement

Search engines of Internet site contents

Examples: www.google.com, www.itools.com, www.aks.com, www.yahoo.com,

Open source intelligence requires a certain degree of specialization. As remarked by experts, the effective use of the internet to gather information is a specialized area of work, and secure methods of searching must be employed so as not to compromise operations.[49]

Intelligence in this sector requires different skills, such as the ability to analyze aggregate information. As it has been pointed out, "the information obtained from open sources tends to fall into two categories, namely one involving information about individuals, and, secondly, involving aggregate information. The aggregate information available is extensive which is where the skills of a qualified analyst come into play as it is a real challenge to assess what is reliable and what is relevant for the purposes of constructing intelligence. Consider some of the new databases, often commercially available, which are able to provide enormous detailed analysis of current trends, companies and individuals. It is no surprise therefore that law enforcement agencies are now increasingly using these methods".[50]

❖ Legal issues

From a law enforcement perspective, one of the values of open source information is that it can be usually searched for and collected without a legal process. However, it raises important legal issues, i.e. civil rights issues related to the retention of open source information for the intelligence process.

Agencies must be vigilant in the managing of open source information because of the regulatory framework that might apply to information retention in a criminal intelligence records system. Indeed, when information is being gathered via open source and is being retained as intelligence, human and constitutional rights claims may arise.

Open source can lead to the mining of important and sensitive information about an individual, for example, a person's credit rating. Therefore, once the information is retained and forms part of an intelligence assessment and a file, questions and processes need to be carefully considered to ensure compliance with the broader issues under human and constitutional rights.[51]

The key is not the source of the information but what is being retained and how it is being retained. On a general basis, it is possible to operate a distinction among raw information obtained from open sources into two categories, where only the first one can raise civil rights issues and therefore requires to be specifically addressed:[52]

Information about individuals and organizations

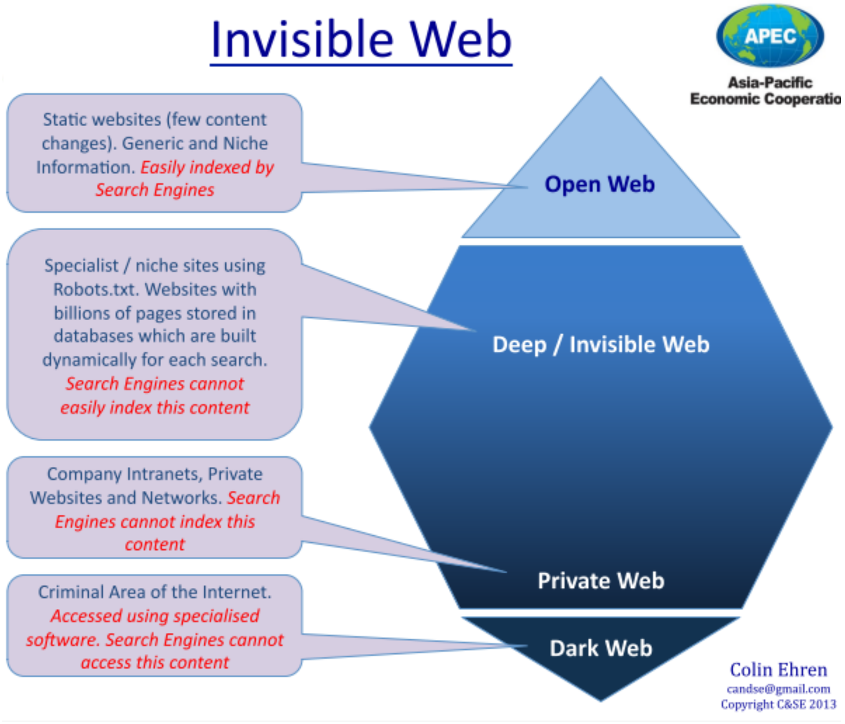
As a general rule, when a law enforcement agency conducts an open source search for information, the agency should assume that civil rights protections attach to any information that identifies individuals or organizations, no matter how innocuous that individual piece of information appears to be.

Aggregate non identifying information

As a general rule, usually no civil rights attach to aggregate information or descriptions of issues, trends, ideologies, and so forth that does not identify an individual or organization.

b. Search Engines and the Deep, or Invisible Web

Currently, hundreds of search engines are available to retrieve information from the internet. However they can easily index only the "Open web", i.e. static websites, with generic and niche information. This is just the tip of the iceberg that represents the information present on the internet.



Invisible Web

Asia-Pacific Economic Cooperatio

Static websites (few content changes). Generic and Niche Information. *Easily indexed by Search Engines*

Open Web

Specialist / niche sites using Robots.txt. Websites with billions of pages stored in databases which are built dynamically for each search. *Search Engines cannot easily index this content*

Deep / Invisible Web

Company Intranets, Private Websites and Networks. *Search Engines cannot index this content*

Private Web

Criminal Area of the Internet. *Accessed using specialised software. Search Engines cannot access this content*

Dark Web

Colin Ehren
candse@gmail.com
Copyright C&SE 2013

Picture taken from: EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

There exists another part of the web, usually referred to as the "deep" or "invisible" web. Deep web is the vast repository of information, that search engines and directories do not have direct access to. It is described as the specialist/niche sites using robots.txt, websites with billions of pages stored in databases, which are built dynamically for each search. Information in databases is generally inaccessible to the software spiders and crawlers that create search engine indexes.

This part of the web can visually be represented by the underwater part of an iceberg, and constitutes the mayor part of the information stored on the web. Common estimates suggest that the deep web contains 500 times the content that is found in the visible web.

In July 2001 it was found that:[53]

- deep web is 400 to 550 times larger than the World Wide Web;
- 7,500 terabytes of information compared to 19 terabytes on WWW.
- 550 billion documents compared to 30 billion on the WWW.
- 200,000+ deep Web sites.

- 60 of the largest sites collectively contained over 40x the information on the WWW.

The deepest part of the iceberg represents “Private Web”, i.e. company intranets, private websites and networks, and the “Dark web”, the criminal area of the web, which is only accessible through specialized software. Neither of the two can be indexed and accessed by search engines.

Five broad types of content constitute the invisible web:[54]

The content of web-based databases

Information stored in databases is accessible only by query to the database and is not picked up by the web crawlers used by search engines. This is distinct from static, fixed web pages, which contain documents that can be accessed directly. A significant amount of valuable information on the web can be generated from databases.

Non-textual files

These include multimedia files, graphics files, software, and documents in formats such as Portable Document Format (PDF). Web crawling has a limitation in searching the content of these types of files. Web crawlers can identify file names and extensions (e.g., .jpg, .wmv, .pdf, etc.) of such files, but cannot identify the content of these files during the web crawling process. Essentially, these files are not in HTML 90 format, therefore a great deal of information and data is not picked up from these files by traditional searches.

Script-based web pages

These are web pages that are written in script coding, other than HTML and/or those with URLs 91 that contain a “?”.

Content available on sites protected by passwords or other restrictions

The content of web sites protected by some degree of access through rigorous password protection or a Virtual Private Network (VPN) will not be identified by search engines. There is a continuum of identifiable and non-identifiable information from these types of web sites depending on what types of information the site owners elect to be publicly accessible (often for marketing purposes) as well as the degree of security applied to the site (in some instances the web site’s security is limited and some data can be identified). A significant amount of information from these sites is not identifiable through traditional search engines.

Pages deliberately excluded by their owners

A web page creator who does not want his or her page captured in search engines can insert special meta tags that will cause most search engines' crawlers to avoid the page.

Search Engines cannot easily index this content, but that doesn’t mean that deep web is not searchable. Investigators must rely on tools that can locate valuable open source deep web information.

The most effective ways to search the deep web is to use search utilities that are designed to explore specific databases. While this still reaches only a portion of the deep web, the information gained from these databases can be extremely valuable. Deep web searching of databases typically requires accessing a variety of web sites to search for the desired information.

What should be apparent is that much of the deep web is not hidden in a surreptitious manner. Rather, it is hidden because it contains information in formats or architectures that are not readily identifiable by standard search engine technologies. As a result, it takes specially designed search utilities and greater effort by the user to identify and capture deep web information.[55]

It should be noted that Internet service providers and companies that operate social networking web sites typically have a published policy and guidance to work specifically with law enforcement agencies.[56] However, when the process goes beyond information that is openly available on the Internet, it is technically not open source information. This issue will therefore be addressed in Section IV. B. 4.

c. Social Media

Social media is a category of the internet-based resources that allows users to generate their own content and then share that content through various connections.[57] It is, at its core, a tool for communication that focuses on integration, collaboration, and interaction, and that has become an integral part of daily life for people of all ages. Social media accounts for 22% of time spent on the internet.[58]

The use of social media in policing is an issue that has only begun to emerge in the last few years. In a recent survey of 800 law enforcement agencies in the United States, 88 percent of agencies reported using social media.[59] According to a July 2012 survey by LexisNexis Risk Solutions, of 1,221 U.S. federal, state, and local law enforcement agencies that use social media in some way, four out of five agencies said they use social media for investigations.[60] The top use is for crime investigations, followed by crime anticipation. Agencies may use social media as an investigative tool when seeking evidence or information about a wide range of criminal activities.[61]

Social networking sites provide a multitude of information about individuals and persons with whom they interact. Social media sites contain identity information of the user and his or her contacts, often with photographs, as well as private messages and statements about beliefs and behavior. While some information, such as a private message, is subject to legal process, a great deal of information is available as an open source.[62]

Examples of social media include blogs, social networking sites, microblogging sites, photo- and video-sharing sites, location-based networks, wikis, mashups, RSS feeds, and podcasts.[63]

- **Facebook** (www.facebook.com)

Social networking site launched in 2005 that lets users create personal profiles describing themselves and then locate and connect with friends, co-workers, and others who share similar interests or who have common backgrounds. Individual profiles may contain—at the user's discretion— detailed personal information, including birth date, home address, telephone number, employment history, educational background, and religious beliefs[64]. Users can also instantly share their exact geographical location by using the "check-in" option. Facebook claimed to have 955 million monthly active users worldwide at the end of June 2012.[65]

- **Twitter** (www.twitter.com)

Social networking site that allows users to share and receive information through short messages that are also known as "tweets." These messages are no longer than 140 characters in length. Twitter users can establish accounts by providing a limited amount of PII but may elect to provide additional personal information if they wish. Users can post messages to their profile pages and reply to other Twitter users' tweets.[66] Users can "follow" other users as well—i.e., subscribe to their tweets. In March 2011, Twitter reported facilitating the delivery of half a billion tweets every day.[67]

- **YouTube** (www.youtube.com)

Online video community that allows users to discover, watch, upload, comment on, and share originally created videos. Similar to Twitter, users can establish accounts on YouTube with only limited amounts of personal information, although they may choose to provide more detailed information on their profile page. Users can comment on videos posted on a page either in written responses or by uploading their own videos. According to YouTube, during 2010 more than 13 million hours of video were uploaded.[68]

❖ **Other commonly used social media**

LinkedIn: www.linkedin.it

Google Groups: groups.google.com

Yahoo Groups: groups.yahoo.com

Windows Live Messenger: messenger.live.com

Skype: www.skype.com

Yahoo Messenger: messenger.yahoo.com

MySpace: www.myspace.com

Orkut: www.orkut.com

Internet Relay Chat

Usenet Talk Groups

Dedicated Discussion Forums

Dating sites (Muslim Match, Uniform Match, Adult Friend, etc.)

Reunion Sites

i. Social Media Monitoring Tools

Law enforcement agencies can rely on social media monitoring tools to capture data and monitor social media sites. These tools offer the ability to search for keywords and thus enable law enforcement to aggregate large amounts of data and refine them into smaller items of interest.[69] For example:

Twitterfall

Netbase

Trackur

CrowdControlHQ

Socialpointer

ii. Compromise Issues & Internet Footprints

There exist multiple ways to access the internet, nonetheless it is recommendable that all detailed or sensitive internet research or open source investigations should be undertaken on a covert or unattributed and registered PC, using a covert or unattributed internet connection. That's because the agency internet footprint could compromise an investigation or an intelligence operation.[70]

If both a covert and a not-covert user search for the same target, the covert user may then be linked to the not-covert user and therefore recognized as an investigator.

Web pages can include images or adverts from third parties, which can leave cookies on your PC. Companies such as "Ad-Image.com" are able to compile a significant profile on you and your surfing habits, which are traded or sold to partners or customers.

iii. Storage of data and gathering of evidence

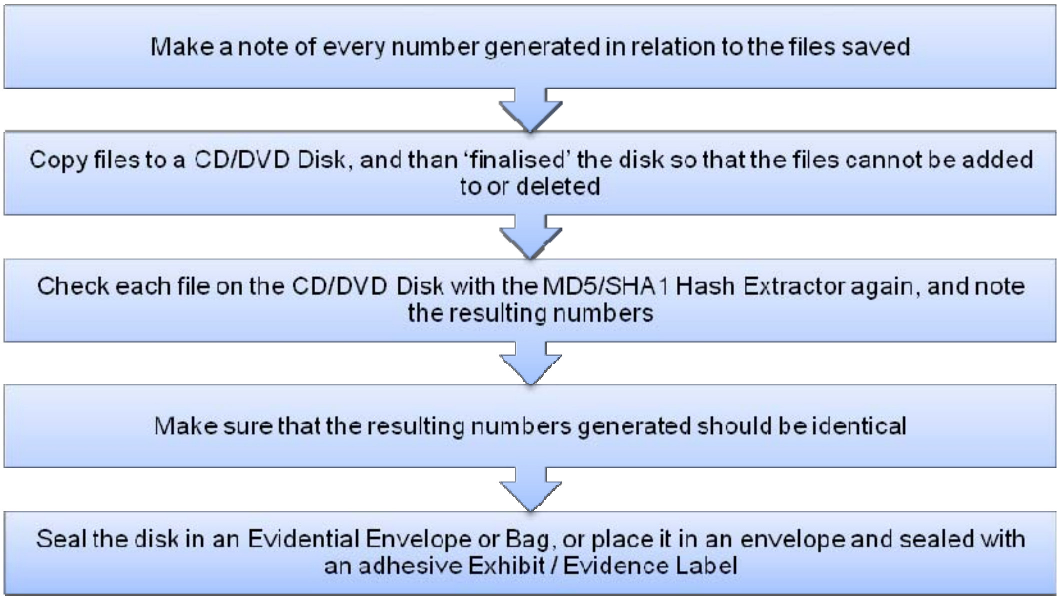
To ensure that a social media investigation can produce high-quality, actionable intelligence, agencies must consider a number of issues, including which types of online content should be viewed and who will conduct the observation and analysis.[71]

Agencies might have to deal with a huge amount of data, and should count on social media extraction and visualization tools.

Many different laws may govern law enforcement agency records. Agency policy should cover the documentation, storage, and retention of social media information gathered for criminal investigations. Information gathered from social media sites should be printed and electronically archived.[72]

When saving and moving data the investigators must ensure that the evidential chain is preserved, in order to use the information as a proof.

In order to preserve the evidential chain, experts recommend making use of an MD5 or SHA1 Hash Extractor, software that retrieves the MD5 hash value (the digital "thumbprint") from files:[73]



Make a note of every number generated in relation to the files saved

Copy files to a CD/DVD Disk, and than 'finalised' the disk so that the files cannot be added to or deleted

Check each file on the CD/DVD Disk with the MD5/SHA1 Hash Extractor again, and note the resulting numbers

Make sure that the resulting numbers generated should be identical

Seal the disk in an Evidential Envelope or Bag, or place it in an envelope and sealed with an adhesive Exhibit / Evidence Label

iv. Privacy and other precautions

Law enforcement must avoid even any appearance of collecting intelligence or information on individuals or organizations due to religious, political, or social views, or on any other grounds that could be regarded as violating the right against discrimination. Collecting data exclusively for those reasons destroys community trust and confidence in law enforcement. Agencies must not use social media to collect information without understanding and following basic civil rights protections. Many agencies already have policies to protect civil rights and civil liberties. Agencies should include references to agency privacy protections when drafting social media policies to collect intelligence and investigate crimes.[74]

Table 8: Judicial decisions - US court precedent

SOURCE: Community of Police Services (COPS) and the Police Executive Research Forum, *Social Media and Tactical Considerations For Law Enforcement*, May 2013, p. 11.

In the United States, one key issue is whether information posted on social media sites such as Facebook is constitutionally protected as private under the Fourth Amendment, and if it is constitutionally permissible for police to set up fictitious identities in Facebook accounts or other social media in order to obtain photos, videos, and other content posted by other Facebook users.

In one case filed on August 10, 2012, the U.S. District Court for the Southern District of New York held that the government did not violate the Fourth Amendment of the USA Constitution when it accessed information from a suspect's Facebook profile that the suspect classified as "private" under the Facebook privacy settings he chose for his Facebook account[75]. The government obtained the information with the assistance of a cooperating witness who had been "friended" by the suspect, and who thus had access to the potentially incriminating information, which included messages about past acts of violence and threats of new acts of violence against rival gang members.

"[The suspect's] *legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the Government*" the court said.

Table 9: *Best Practices - Social Media policies*

See the Georgia Bureau of Investigation social media policy entitled "Guidelines for the Use of Social Media by the Investigative Division", attached as Appendix B to the Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013), 29–35, at

www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf

2. Government agencies databases (publicly and not-publicly available)

In many economies, local and state agencies maintain websites publicly available on-line, where general public can retrieve information, because policy, regulation, or the law permits the custodian of such information to do so. Users, and so investigators, are allowed to access hundreds of sources of current government information – such as census data, judicial decisions, property and vehicle ownership records, property ownership, lien filings, company financial reports, salaries of public employees – and a wide array of other information for which an individual has little, if any, control over its public release.[76]

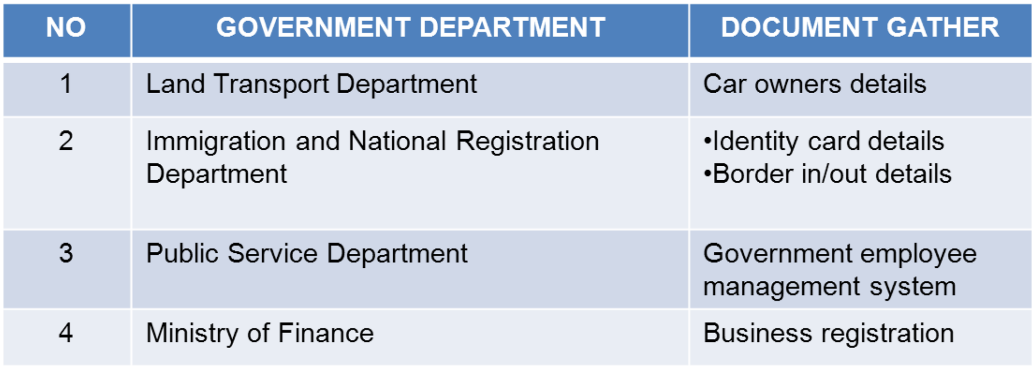
Other public agencies and departments maintain registers not accessible to the general public, but may allow law enforcement agencies to access their databases, either directly, or through the appropriate administrative or judicial process.

When instant access is not guaranteed, but Courts routinely grant access, a useful practice may be that of stipulating MoUs with different government departments to such end.

Table 10: *Best practices - Brunei Darussalam ACB Intelligence Section*

SOURCE: Anti-corruption Bureau, Prime Minister's Office, Brunei Darussalam, "The Use of IT Resources for Evidence Gathering and Analysis", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

The ACB Intelligence Section has a Memorandum of Understanding for information sharing with several government departments. The mode of sharing information is by system link. The departments that have approved the MoU and the documents shared with the ACB are the following:



NO	GOVERNMENT DEPARTMENT	DOCUMENT GATHER
1	Land Transport Department	Car owners details
2	Immigration and National Registration Department	•Identity card details •Border in/out details
3	Public Service Department	Government employee management system
4	Ministry of Finance	Business registration

Financial information retrievable from public databases can be of high value for investigators. There are a great number of databases that could be used by a prosecutor or investigator in a corruption case.

Given that a suspect frequents a certain residence, for example, public records could allow investigators to ascertain the ownership of the house, when it was bought, from whom and for how much, how the payment took place and who is paying taxes on it. As for corporations, public registers permit to gather information about when and where the company was formed, who are its directors or officers, and many other data.

- **Public Databases and Records**[77]

Firearms Registries

Can provide information about liquor, firearms, and explosives licensing

Drug Enforcement Administrations

Can provide investigators with relevant case data, information on individuals and companies related to cases, known assets, business and financial information related to cases, analytical databases for the analysis of telephone number information, etc.

Financial Information Units

Can provide analytical research services, databases for evidence or leads to relationships between subjects and other persons or entities, link analysis to show connections, Suspicious Transaction Reports and many other financial information.

Tax agencies and Tax records

Can provide information on Sales and use tax, Personal property tax, Real property tax, Business license tax, Income tax, Gift tax, Inheritance tax, etc.

INTERPOL

Can provide access to international networks of criminal activity files, query by name or business name, and provide intelligence checks to complete a file.

Crime and Law Enforcement Information Centers and Networks

Provide information on criminal history, Fingerprints, Vehicles, License plates, Securities, Boats, Guns, Wanted persons (domestic and foreign), Unidentified persons files, criminal history records

Custom Service

Information on people and goods.

Companies public registries

Information on all corporations incorporated or doing business, ownership, corporate bylaws, capital, credit reports, information on corporate mergers, reorganizations and consolidations. Identification information on all partnerships and professional associations formed or doing business.

Securities Supervisors

Information about issuers, company reports and disclosures, history of dividends, stock splits, and key financial ratios; proxy statements, enforcement actions, change in registrant's certifying accountant, details of stock acquisition, source of money used to buy stock, corporate documents, documents from third parties

Bankruptcy Records

Information about bankruptcy, assets at time of bankruptcy, creditors at time of

bankruptcy.
Often provides an excellent starting point for net worth purposes and leads to hidden assets

Civil and Criminal Court Records
Information on Civil suits and Criminal actions.
Can provide leads to hidden transactions or assets revealed through civil suits; leads to witnesses who may be hostile to the subject; leads to aliases and previously unknown addresses; leads to previously unknown affiliations with other persons or entities

Divorce and Legal Separation Records
Leads to: hidden transactions or assets revealed through divorce proceedings, witnesses who may be hostile to the subject, previously unknown affiliations with other persons or entities

Automobile License Departments or Agencies
Owner's name, Vehicle identification number, Physical description of listed automobiles

Drivers License Bureau Departments or Agencies
Driver's name, date of birth, physical description, and address, License renewal date and the type of license issued

Professional and Commercial Licenses
Information about Medical, Dental, Insurance agency, Stock broker, Real estate broker, Attorney, Certified Public Accountant, Concealed weapons, Gun permits, Liquor, Notary Licenses

Real Estate Records
Building Permit records: may reveal hidden property, payments by third parties for improvements on property, leads to previously unknown affiliations with other persons or entities, evidence of beneficial ownership of the property
Grantor and Grantee Records: Deeds, Real estate agreements, Liens and lien releases, Real estate and chattel mortgages, Options to buy, Easements and easement releases.
Maps and Plats: compare county maps and plats with aerial photos, measured mileage, surveillance notes, etc.
Liens Register: may reveal new construction, property improvements, hidden property, payments by third parties for improvements on property, leads to previously unknown affiliations with other persons or entities, evidence of beneficial ownership of the

property
Tax Assessor's Records: may indicate separate assessed values for land and improvement, cross reference property by legal description, who pays taxes on the property, address where the property tax bills are being sent, may cross-reference other properties whose tax bills are being sent to same address, may cross-reference other properties on which subject is paying taxes, may provide previously undisclosed relationships with other persons or entities, may provide evidence of beneficial ownership of the property

Gaming Departments or Agencies
Owners of gaming establishments, names of persons banned from gaming establishments, financial information on gaming establishments

Civil registries
Births, Deaths, Adoptions

Trade Name Index
Trade names of businesses, including corporations, partnerships, professional corporations and sole proprietorships doing business in the region; Addresses of businesses, Name, address and identity of owners.

Bureau of Public Debt
Cash purchases of Treasury bills

Coast Guard
Records of vessels

Ministries of Interior / State Departments or similar
ID Records, Passport records, Visa records

Aviation Administration
Information on aircraft, owners and previous owners, serial number, model, information on licensed pilots

Immigration Departments
Identification information on immigrants and aliens, lists of passengers and crews on vessels from foreign ports, naturalization records, deportation records, financial statements of aliens and persons sponsoring their entry.

Postal Service
Postal money orders, Addresses, Mail covers

Trash Searches
Records obtained by searching through subject’s trash

Utility Companies
Water, Sewer, Trash hauling, Electricity, Gas, Telephone.
Leads to third parties, principals, and hidden assets: may reveal third parties who are paying the bills, bills on other properties being paid by the same person or company, previously undisclosed bank accounts from which bills are being paid, leads to hidden property on which bills are being paid

Chapter IV: The Gathering of Private digital sources of evidence and the use of digital forensic tools

Nowadays, large parts of human activities create some type of digital evidence.[78] Back in 2001, a study by the University of California-Berkeley already pointed out that at least 93% of all new information was created in digital format;[79] while back in 1998, 3.4 trillion e-mail messages were sent across the world.[80] Since then those figures have increased dramatically: in 2007, it was reported that more electronic documents were created worldwide in the prior year than the printed documents in all the years combined since Gutenberg invented the printing press.[81]

In 2013, 3.9 billion email accounts have been reported, with the business mailboxes accounting for the 24% of the total. The majority of email traffic comes from business emails, which account for over 100 billion emails sent and received per day.[82]

However, digital evidence is not associated only with creating an email or writing a document with a computer. Surfing the internet or driving a car with the GPS, paying a bill or using a video camera, withdrawing cash or using a copy machine: each of these actions creates digital evidence, and even activities that are perceived as not producing electronic evidence are eventually digitized at some point.[83]

Significant digital sources of evidence in the investigation of corruption cases include:

Computers
Mobile devices
Removable media and external data storage devices
Online banking software
Calendar(s)
E-mail, notes, and letters
Telephone records
Financial or asset records
Electronic money transfers
Accounting or recordkeeping software

Table 11: *Hong Kong, China - How do we use IT resources?*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

- Data acquisition, recovery, preservation and examination
- Computer
  - Email
  - Document file…
- Mobile phone
  - Call history
  - Contact list
  - Short message
  - Email
  - Photo
  - WhatsApp

The importance of this enormous amount of evidence is that it can be recovered and used in criminal investigations, in asset tracing and in any legal proceedings. Doing so requires a process of collection, preservation and analysis of electronic data that must then be presented for use in a litigation process.

Forensic acquisition and analysis of data techniques combine lost and tampered data with other digital evidence, allowing for easier identification, collection, preservation, analysis and presentation of evidence generated or stored in a computer.[84]

Additionally, as much of the day-to-day communication and financial transactions are conducted over the Internet, real time monitoring of bank accounts, e-mail traffic and the interception and processing of other forms of on-line data become essential for conducting a proper investigation, complementing traditional investigative and surveillance techniques.[85]

Since all these activities require the assistance of a digital forensic expert, the increasing trends have led to a huge demand for highly educated specialists in these disciplines.[86]

DIGITAL EVIDENCE: Definition

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, U.S. Department of Justice-Office of Justice Programs, Washington, 2008, p. ix

Electronic evidence originates when electronic data regarding some type of activity or transaction are stored somewhere, where they might be accessed and recovered by a forensic examiner.

Today digital evidence can be found on everything from floppy disks to media cards, solid-state memory sticks, solid-state hard drives, cell phones, network attached storage devices, game consoles, media players, hard drives, and the "Internet cloud.

L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom*, Waltham, 2012, p. 5

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

G. PALMER, *A Road Map for Digital Forensic Research*, DFRWS 16, Nov. 6, 2001

Digital Forensic makes use of different methods and techniques, in order to deal with a variety of issues and to meet the diverse needs of criminal investigations. It is possible, however, to summarize four essential elements or principles upon which every digital forensic technique relies on.[87]

Acquisition

The process of actually collecting electronic data, such as seizing a computer at a crime scene or making a forensic copy of ("acquiring" in the forensic language) a computer hard drive.

It is the first step in the forensic process and is critical to ensure the integrity of the evidence, since it is the moment where evidence is most likely to be damaged or destroyed.

Preservation

The process of creating a chain of custody that begins prior to collection and ends when evidence is released to the owner or destroyed.

It includes keeping the evidence safe from intentional destruction by malicious persons or accidental modification by untrained personnel.

Analysis

The process of locating and collecting evidentiary items from evidence that has been collected in a case. It includes the identification of target information (such as financial records, for example) as well as the use of specific forensic tools.

Presentation

The activity of presenting the examiner's findings is the last step in the process of forensic analysis of electronic evidence. This includes not only the written findings or forensic report, but also the creation of affidavits, depositions of experts, and court testimony.

Table 12: *Hong Kong, China - Challenges*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

<ins>Technical difficulties</ins>

- Cloud computing
  - Information and evidence are remotely stored
  - Liaison with online service providers
- Huge data size
  - Storage Area Network (SAN) to keep forensic image
- Data encryption
  - Password cracking tool
  - Chip level data acquisition

Admissibility of digital evidence

- Local digital evidence
- Foreign digital evidence
- Expert opinion on chain of evidence
- Admissibility of evidence in court trials

A. Best practices for handling digital evidence

In dealing with digital evidence, law enforcement agencies must ensure that adequate procedures are in place, since every activity of the law enforcement personnel exposes the evidence to the risk of accidental modification. That's the reason why, in ensuring that evidence will be accepted in a court of law as being authentic and an accurate representation of the original evidence, the moments of collection and preservation of evidence are extremely critical.

Modification of evidence can have a devastating effect on the entire case, and therefore digital evidence needs to be protected and preserved all along the process collection, acquisition, analysis and presentation.

In the implementation of proper procedures and in the elaboration of training programs, agencies must apply the following general forensic principles:[88]

- The process of collecting, securing, and transporting digital evidence should not change the evidence;
- Digital evidence should be examined only by those trained specifically for that purpose;
- Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.

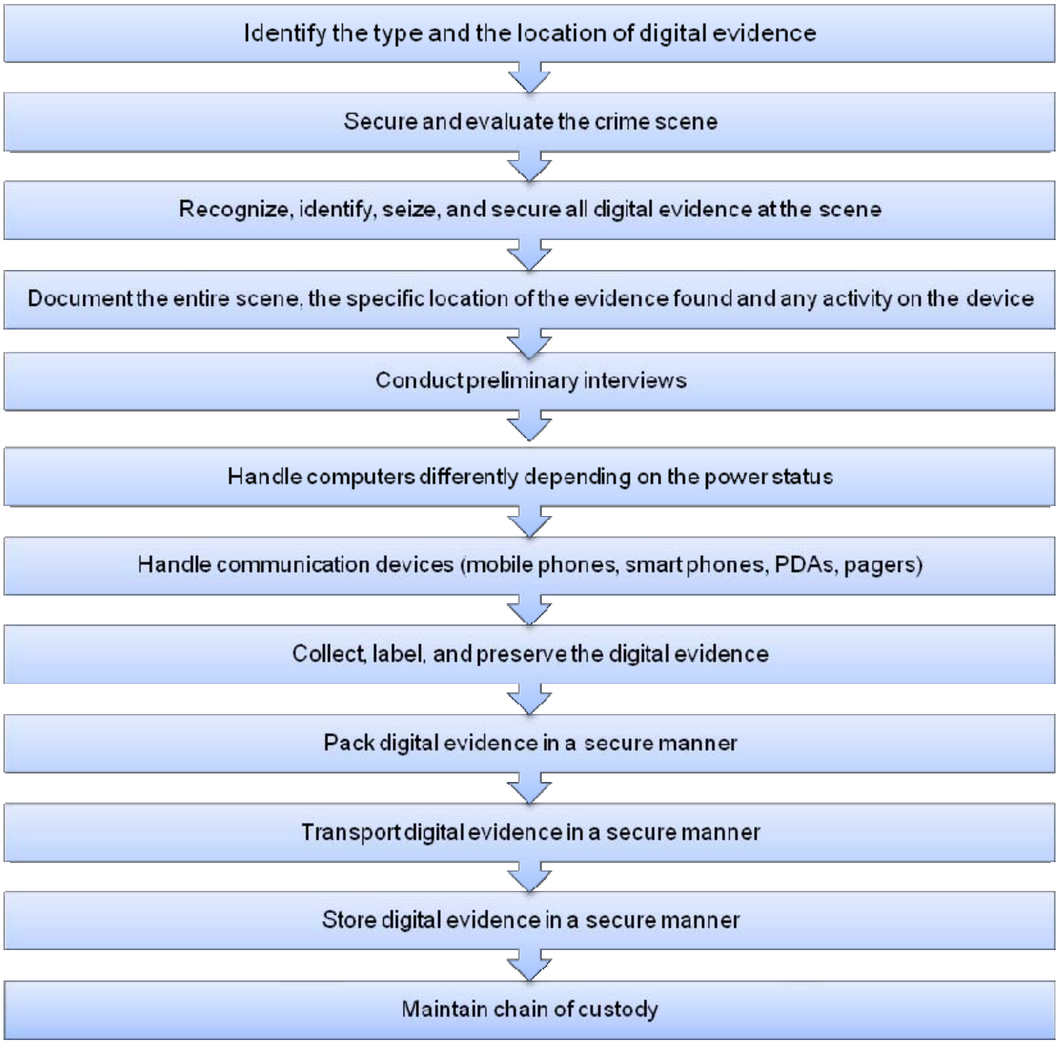
In the following sections, models are presented of those protocols and procedures that every agency should put in place for each critical stage in the digital evidence gathering process.[89]

1. Collection and preservation of digital evidence

The collection step is critical since this is the first real contact with evidence. Not following proper collection procedures can lead to the destruction or modification of evidence, lost evidence, and subsequent challenges of the evidence collected.[90] Some digital evidence requires special collection, packaging, and transportation techniques.

Indeed, data can be damaged or altered by electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.[91]

The following chart summarizes all activities that must be performed in the process of acquisition. Each activity will be detailed below.


Identify the type and the location of digital evidence
Secure and evaluate the crime scene
Recognize, identify, seize, and secure all digital evidence at the scene
Document the entire scene, the specific location of the evidence found and any activity on the device
Conduct preliminary interviews
Handle computers differently depending on the power status
Handle communication devices (mobile phones, smart phones, PDAs, pagers)
Collect, label, and preserve the digital evidence
Pack digital evidence in a secure manner
Transport digital evidence in a secure manner
Store digital evidence in a secure manner
Maintain chain of custody

1	**Identify the type and the location of digital evidence**
□	Include any location and item in which digital evidence may reside in preparing or applying for a search warrant.
□	Determine the necessary equipment to take to the scene
□	Review the legal authority to collect evidence, ensuring any restrictions are noted.

Warning

Collecting items not previously identified can cause that evidence to be suppressed in a legal action. Identification language must be specific and must have correct terminology; using language such as “CPU” instead of computer would mean that you can collect only the Central Processing Unit of a computer and not the computer itself.

2 Secure and evaluate the crime scene

□ Follow departmental policy for securing crime scenes.

□ Ensure that no unauthorized person has access to any electronic devices at the crime scene.

□ Refuse offers of help or technical assistance from any unauthorized persons.

□ Remove all persons from the crime scene or the immediate area from which evidence is to be collected.

3 Recognize, identify, seize, and secure all digital evidence at the scene

□ Search the scene systematically and thoroughly;

□ Immediately secure all electronic devices, including personal or portable devices.

□ Ensure that the condition of any electronic device is not altered.

□ Leave a computer or electronic device off if it is already turned off.

□ Consider the possibility of anti-forensic techniques (such as destructive devices and wiping software)

4 Document the entire scene

□ Record the location of the scene, the state, power status, and condition of computers, storage media, wireless network devices, mobile phones, smart phones, PDAs, and other data storage devices; Internet and network access; and other electronic devices;

□ Photograph the evidence in place prior to collection or duplication;

□ Prepare a complete inventory of each item including identifying information such as serial numbers, manufacturer, and descriptions;

□ Record all activity and processes on display screens

□ Record all physical connections to and from computers

□ Record any network and wireless access point that may be present

□ Do not move electronic devices until they are powered off

5 Conduct preliminary interviews

In conformity with applicable laws and regulations, investigators should ask all adult persons of interest at the crime scene for the following information:

☐ Names of all users of the computers and devices.

☐ All computer and Internet user information.

☐ All login names and user account names.

☐ Purpose and uses of computers and devices.

☐ All passwords.

☐ Any automated applications in use.

☐ Type of Internet access.

☐ Any offsite storage.

☐ Internet service provider.

☐ Installed software documentation.

☐ All e-mail accounts.

☐ Security provisions in use.

☐ Web mail account information.

☐ Data access restrictions in place.

☐ All instant message screen names.

☐ All destructive devices or software in use.

☐ MySpace, Facebook, or other online social networking Web site account information.

☐ Any other relevant information

6 Handle computers differently depending on the power status

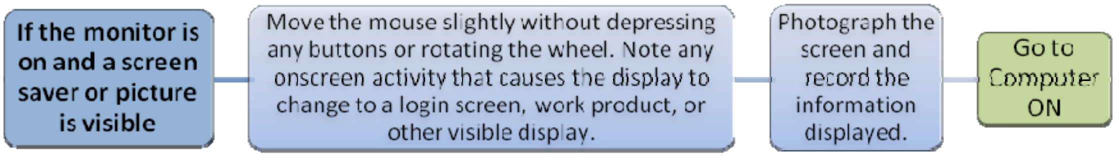
If someone attempts to collect a device and does not understand the proper methods to shut down the computer, operates the computer prior to shutdown, or shuts down a critical business server improperly, it can lead to data loss, civil liability for lost business, and the loss of critical evidence that could be collected prior to shut down.

6.1 Assess the Situation

☐ Look and listen for indications that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes

	(LEDs) are on.
□	Check the display screen for signs that digital evidence is being destroyed. Words to look out for include “delete,” “format,” “remove,” “copy,” “move,” “cut,” or “wipe.”
□	Look for indications that the computer is being accessed from a remote computer or device.
□	Look for signs of active or ongoing communications with other computers or users such as instant messaging windows or chat rooms.
□	Take note of all cameras or Web cameras (Web cams) and determine if they are active
□	Look and listen for indications that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes (LEDs) are on.

6.2 Identify the computer’s power status

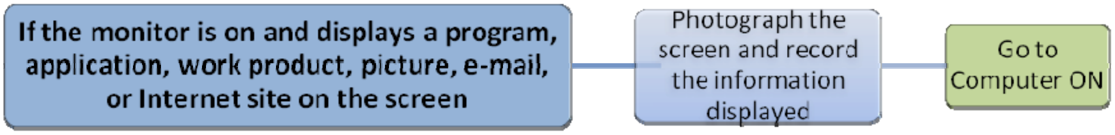


If the monitor is on and a screen saver or picture is visible

Move the mouse slightly without depressing any buttons or rotating the wheel. Note any onscreen activity that causes the display to change to a login screen, work product, or other visible display.

Photograph the screen and record the information displayed.

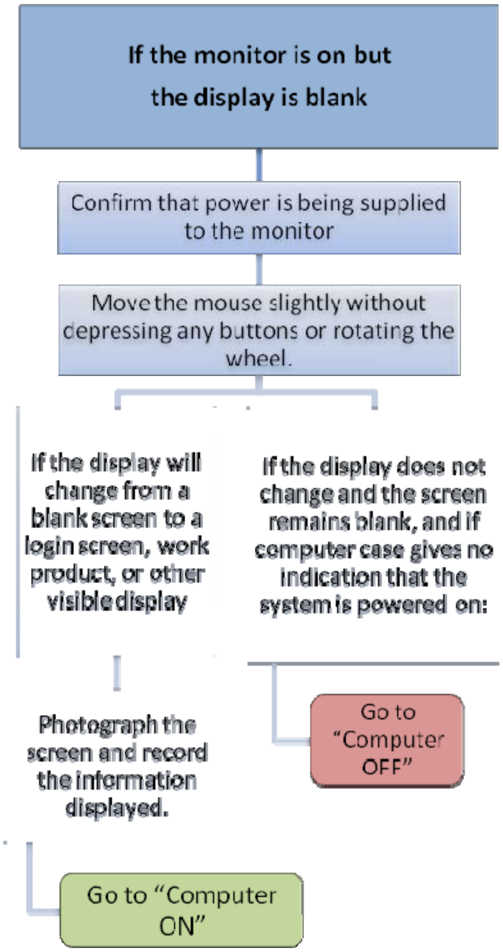
Go to Computer ON

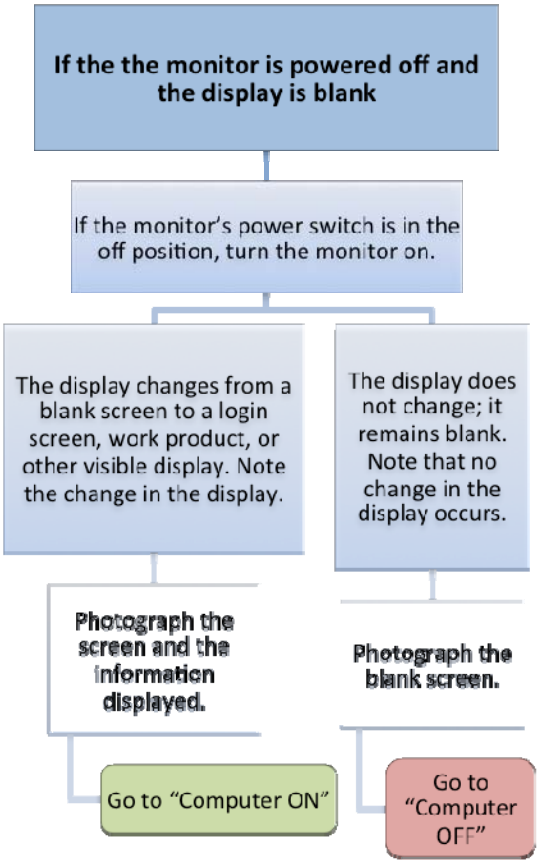


If the monitor is on and displays a program, application, work product, picture, e-mail, or Internet site on the screen

Photograph the screen and record the information displayed

Go to Computer ON


If the monitor is on but the display is blank
Confirm that power is being supplied to the monitor
Move the mouse slightly without depressing any buttons or rotating the wheel.
If the display will change from a blank screen to a login screen, work product, or other visible display
If the display does not change and the screen remains blank, and if computer case gives no indication that the system is powered on:
Photograph the screen and record the information displayed.
Go to "Computer OFF"
Go to "Computer ON"


If the the monitor is powered off and the display is blank
If the monitor's power switch is in the off position, turn the monitor on.
The display changes from a blank screen to a login screen, work product, or other visible display. Note the change in the display.
The display does not change; it remains blank. Note that no change in the display occurs.
Photograph the screen and the information displayed.
Photograph the blank screen.
Go to "Computer ON"
Go to "Computer OFF"

6.3 Computer OFF

For desktop, tower, and minicomputers follow these steps:

□ Document, photograph, and sketch all wires, cables, and other devices connected to the computer.

□ Uniquely label the power supply cord and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire, or USB drive occupies on the computer.

□ Photograph the uniquely labeled cords, cables, wires, and USB drives and the corresponding labeled connections.

□ Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip, or battery backup device.

□ Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.

□ Place tape over the floppy disk slot, if present.

□ Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.

□ Place tape over the power switch.

□ Record the make, model, serial numbers, and any user-applied markings or identifiers.

□ Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.

□ Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

For laptop computers follow these steps:

□ Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.

□ Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.

□ Photograph the uniquely labeled cords, cables, wires, and devices connected to the laptop computer and the corresponding labeled connections they occupied.

□ Remove and secure the power supply and all batteries from the laptop computer.

□ Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.

□ Place tape over the floppy disk slot, if present.

□ Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.

□ Place tape over the power switch.

□ Record the make, model, serial numbers, and any user applied markings or identifiers.

□ Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.

□ Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

6.4 Computer ON

For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the computer display, however, you may need to request assistance from personnel who have experience in volatile data capture and preservation.

□ Examine the computer for any running processes. If it is observed running a destructive process, the examiner should stop the process and document any actions taken.

☐ Consider Capture RAM and other volatile data from the operating system (**See Box below**)

☐ Determine if any of the running processes are related to cloud or off-site storage. When encountered, the examiner should coordinate with the appropriate legal authority to ensure the scope covers the off-site acquisition.

☐ Document and hibernate any running virtual machines.

☐ Consider the potential of encryption software installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the unencrypted data before the computer is powered off.

☐ Save any opened files to trusted media.

☐ Isolate the computer from any network connectivity.

☐ Use a triage tool to preview data.

☐ Evaluate the impact of pulling the plug vs. shutting the computer down. This is typically dependent upon the operating system and file system encountered.

In the following situations, immediate disconnection of power is recommended

■ Information or activity onscreen indicates that data is being deleted or overwritten.

■ There is indication that a destructive process is being performed on the computer's data storage devices.

■ The system is powered on in a typical Microsoft ® Windows ® environment. Pulling the power from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands,

In the following situations, immediate disconnection of power is NOT recommended:

■ Data of apparent evidentiary value is in plain view onscreen. The first responder should seek out personnel who have experience and training in capturing and preserving volatile data before proceeding.

■ Indications exist that any of the following are active or in use:

- Chat rooms and instant message windows
- Open text documents
- Remote data storage
- Data encryption
- Financial documents

For mainframe computers, servers, or a group of networked computers, the first responder should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems.

Table 13: *Volatile Data*

SOURCE: Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 26.

Some evidence is only present while a computer or server is in operation and is lost if the computer is shut down. Evidence that is only present while the computer is running is called volatile evidence and must be collected using live forensic methods. This includes evidence that is in the system's RAM (Random Access Memory), such as a program that only is present in the computer's memory. These programs are considered TSRs or Terminate and Stay Resident programs. […] There are also many types of other volatile evidence that are only available while the computer is running, including certain temporary files, log files, cached files, and passwords. RAM is cleared when the computer is turned off and any data that is present is lost. This can be a critical step if there is suspicion that any kind of data encryption is enabled that prevents the hard drive or portions of the hard drive from being viewed. In many cases the only way to recover the password needed to remove the encryption on a hard drive is to collect the "live memory" before the computer is turned off. Also, if the computer is running, the encrypted portion of the data storage would be accessible, but only until the computer is turned off, making it essential that the hard drive is copied while the computer is still turned on. There are tools available to make copies of RAM and hard drives on running computers and line-of-business servers that cannot be shut down, and still ensure that those copies are forensically sound.

Table 14: *Warning - Acquire data from live systems*

SOURCE: Scientific Working Group on Digital Evidence (SWGDE), Capture of Live Systems, 2008, p. 2.

Great care must be taken when attempting to capture or acquire data from live systems. These are advanced techniques that require advanced training and tools to accomplish the desired results while minimizing the possible destruction of data or hardware. If the person attempting to acquire the data is unsure of the methods used to perform the acquisition, then professional assistance should be sought.

There are three methods utilized in live acquisitions:

1. RAM dump

2. Logical copying of files

3. Physical acquisition of the entire system

Each of these can be used independently or in conjunction with others depending on the scope of the search.

7 Communication devices (mobile phones, smart phones, PDAs, pagers)

☐ Secure the devices

☐ Prevented devices from receiving or transmitting data once they are identified and collected as evidence

8 Collect, label, and preserve the digital evidence

☐ Tag each item for tracking and identification.

☐ Secure each item to prevent inadvertent operation. This includes placing tamper-proof tape over power outlets, CD-ROM drives, USB ports, and floppy disk trays.

☐ Bag each item in a forensically sound manner, into a secure container that is sealed with tamper-proof tape to ensure that the evidence is not modified or damaged during transport.

☐ If more than one computer is seized as evidence, all computers, cables, and devices connected to them should be properly labeled to facilitate reassembly if necessary.

9 Pack digital evidence in a secure manner

☐ Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried before it is packaged. All connections and connected devices should be labeled for easy reconfiguration of the system later.

☐ Remember that digital evidence may also contain latent, trace, or biological evidence and take the appropriate steps to preserve it. Digital evidence imaging should be done before latent, trace, or biological evidence processes are conducted on the evidence.

☐ Pack all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes, and antistatic containers should be used for packaging digital evidence. Plastic materials should not be used when collecting digital evidence because plastic can produce or convey static electricity and allow humidity and condensation to develop, which may damage or destroy the evidence.

☐ Ensure that all digital evidence is packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.

☐ Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found.

☐ Package mobile or smart phone(s) in signal-blocking material such as faraday isolation bags, radio frequency-shielding material, or aluminum foil to prevent data messages from being sent or received by the devices.

☐ Collect all power supplies and adapters for all electronic devices seized.

10	Transport digital evidence in a secure manner
☐	Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity.
☐	Keep digital evidence away from magnetic fields such as those produced by radio transmitters, speaker magnets, and magnetic mount emergency lights.
☐	Avoid keeping digital evidence in a vehicle for prolonged periods of time. Heat, cold, and humidity can damage or destroy digital evidence.
☐	Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.
☐	Document the transportation of the digital evidence and maintain the chain of custody on all evidence transported.

11	Store digital evidence in a secure manner
☐	Ensure that the digital evidence is inventoried in accordance with the agency's policies.
☐	Ensure that the digital evidence is stored in a secure, climate-controlled environment or a location that is not subject to extreme temperature or humidity.
☐	Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.
	WARNING: Potentially valuable digital evidence including dates, times, and system configuration settings may be lost due to prolonged storage if the batteries or power source that preserve this information fails. Where applicable, inform the evidence custodian and the forensic examiner that electronic devices are battery powered and require prompt attention to preserve the data stored in them.

12	Maintain chain of custody
☐	Proper check-in and check-out procedures with a maintained chain of custody for any access to or movement of the evidence
☐	Final disposition of the evidence, recorded in the chain of custody for any evidence that is released or destroyed
☐	Each piece of evidence should be protected from damage or alteration, labeled and a chain-of-custody maintained as determined by organizational policy.
☐	Document the transportation of the digital evidence and maintain the chain of custody on all evidence transported.

Table 15: *Best Practices –Hong Kong China - Faraday Bags*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

Mobile devices such as smart phones are kept in radio frequency shielding faraday bags to prevent digital evidence from being interfered with by external communication.

2. Acquisition of digital evidence

Acquisition is the part of the forensic process during which actual data is copied or duplicated. Once again, ensuring the integrity of evidence is the most critical part of the procedure.

a. Duplication

The only accepted method for duplicating electronic evidence requires that the original be protected from any possibility of alteration during the duplication process. This requires the use of accepted tools and techniques that allow the duplication of the evidence in a forensically sound manner.

Forensic methods for duplication

The proper forensic method for duplicating evidence from a computer hard drive or other media storage device requires the use of write-blocking of the original storage device.

Write-blocking can be accomplished either by using a physical hardware device that is connected between the original (source) and the copy (target) hard drive or by using a special boot media that can start a computer in a forensically sound manner.

When is practical to remove the hard drive:

☐ Remove the hard drive from the computer

☐ Connect it to a physical write-blocker

☐ Use a forensic workstation and forensic software to make the copy.

In case it is not practical to remove the hard drive:

☐ Start up the computer in a forensically sound manner (see next box)

☐ Make a copy of the hard drive using a software-based write-blocking method

Table 16: Starting up a computer with a forensic operating system

SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 31.

When a computer is first turned on, it goes through a set of steps, beginning with a Power On Self-Test (POST), followed by loading of the Basic Input Output System (BIOS).

During normal operation, the computer will load the operating system installed on the hard drive, such as Microsoft Windows or the Mac OS. It is possible to prevent the computer from loading the operating system that is installed on the hard drive.

When preparing to perform a forensic copy of a computer's hard drive(s), a forensic examiner would force the computer to load a special forensic operating system from a specially prepared boot media.

This is critical because when a computer starts up (boots) normally from the installed operating system, whether Windows or Mac OS or Linux, these operating systems automatically "mount" the hard drive(s) in read/write mode. [...] These forensic operating systems are modified to effectively turn off the ability of the computer to make any changes to the hard drive(s).

Table 17: *Why not to use a non-forensic duplication method*

SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 30.

Using non forensic methods will always lead to modification of the original evidence and/or incomplete copies of the original evidence that cannot be verified using forensic methods.

Personnel not trained in the proper forensic methods for duplicating electronic evidence may start a computer up and then make copies of the data on the hard drive.

When a computer is started up in this manner, the operating system can write to the hard drive and change file dates, change log files, and other types of files, effectively modifying and destroying critical evidence.

b. Verification

This is the final step in the forensic copy process. In order for evidence to be admissible, it must be possible to verify that the evidence presented is exactly the same as the original collected.

Table 18: *Creating a "hash value"*

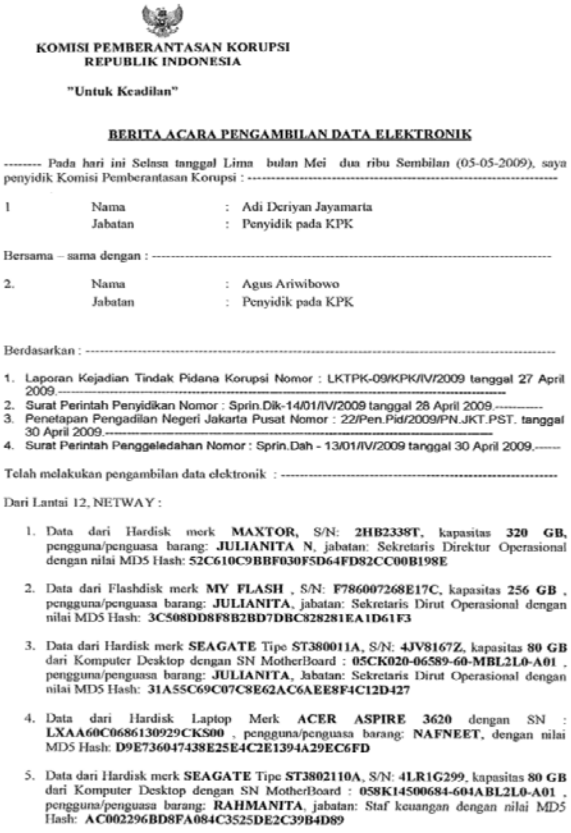
SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 31.

Verification is accomplished by using a mathematical algorithm that calculates a number based on the contents of the evidence. … This is called creating a "hash value" and is performed by using either the Message Digest 5 (MD-5) algorithm or a Secure Hash Algorithm (SHA). The MD-5 is the most commonly used method for verification in computer forensics at this time. Forensic duplication tools automatically create a "verification" hash for the original and the copy during the duplication process. If these hash values do not match, there is an opening for a challenge to the authenticity of the evidence as compared to the original.

Table 19: *Best Practices - The Indonesian Experience of KOMISI PEMBERANTASAN KORUPSI*

SOURCE: Indonesia presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

We include a digital fingerprint in our affidavit when we seize the evidence. This policy is taken to strengthen the validity of the evidence. Thus, the validity of the evidence can be tested by everyone.



KOMISI PEMBERANTASAN KORUPSI
REPUBLIK INDONESIA

"Untuk Keadilan"

BERITA ACARA PENGAMBILAN DATA ELEKTRONIK

-------- Pada hari ini Selasa tanggal Lima bulan Mei dua ribu Sembilan (05-05-2009), saya penyidik Komisi Pemberantasan Korupsi : --

1 Nama : Adi Deriyan Jayamarta
Jabatan : Penyidik pada KPK

Bersama – sama dengan : --

2. Nama : Agus Ariwibowo
Jabatan : Penyidik pada KPK

Berdasarkan : --

1. Laporan Kejadian Tindak Pidana Korupsi Nomor : LKTPK-09/KPK/IV/2009 tanggal 27 April 2009.--
2. Surat Perintah Penyidikan Nomor : Sprin.Dik-14/01/IV/2009 tanggal 28 April 2009.----------
3. Penetapan Pengadilan Negeri Jakarta Pusat Nomor : 22/Pen.Pid/2009/PN.JKT.PST. tanggal 30 April 2009.---
4. Surat Perintah Penggeledahan Nomor : Sprin.Dah - 13/01/IV/2009 tanggal 30 April 2009.-----

Telah melakukan pengambilan data elektronik : ---

Dari Lantai 12, NETWAY :

1. Data dari Hardisk merk **MAXTOR,** S/N: **2HB2338T**, kapasitas **320 GB,** pengguna/penguasa barang: **JULIANITA N**, jabatan: Sekretaris Direktur Operasional dengan nilai MD5 Hash: **52C610C9BBF030F5D64FD82CC00B198E**
2. Data dari Flashdisk merk **MY FLASH** , S/N: **F786007268E17C**, kapasitas **256 GB** , pengguna/penguasa barang: **JULIANITA**, jabatan: Sekretaris Dirut Operasional dengan nilai MD5 Hash: **3C508DD8F8B2BD7DBC828281EA1D61F3**
3. Data dari Hardisk merk **SEAGATE** Tipe **ST380011A**, S/N: **4JV8167Z**, kapasitas **80 GB** dari Komputer Desktop dengan SN MotherBoard : **05CK020-06589-60-MBL2L0-A01** , pengguna/penguasa barang: **JULIANITA**, Jabatan: Sekretaris Dirut Operasional dengan nilai MD5 Hash: **31A55C69C07C8E62AC6AEE8F4C12D427**
4. Data dari Hardisk Laptop Merk **ACER ASPIRE 3620** dengan SN : **LXAA60C0686130929CKS00** , pengguna/penguasa barang: **NAFNEET**, dengan nilai MD5 Hash: **D9E736047438E25E4C2E1394A29EC6FD**
5. Data dari Hardisk merk **SEAGATE** Tipe **ST3802110A**, S/N: **4LR1G299**, kapasitas **80 GB** dari Komputer Desktop dengan SN MotherBoard : **058K14500684-604ABL2L0-A01** , pengguna/penguasa barang: **RAHMANITA**, jabatan: Staf keuangan dengan nilai MD5 Hash: **AC002296BD8FA084C3525DE2C39B4D89**

Table 20: Case example – *Pronosticos* case, the Mexican Experience

SOURCE: Mexico presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

Six public servants at *Pronósticos Deportivos*, a national lottery branch, defrauded the institution for about 110 million pesos. The investigation unit (DGII) investigated the modus operandi and fully identified them.

Computer forensics performed actions:

Phase 1

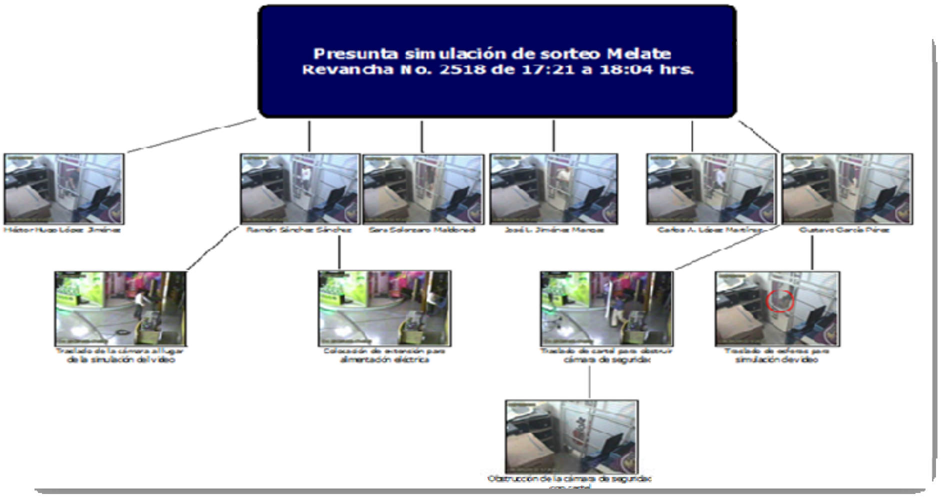
Forensics procedures were applied, like data recovery from computer hard disks where the videos were recorded and edited to manipulate the lottery results.

Phase 2

Forensics procedures were also applied to the surveillance system to get the videos from the day the fraud was made.

Phase 3

The videos were checked sequentially to identify how the public servants managed to trick the results and those results were reported as evidence to ministerial authority.



Presunta simulación de sorteo Melate Revancha No. 2518 de 17:21 a 18:04 hrs.
Héctor Hugo López Jiménez
Ramón Sánchez Sánchez
Sara Solorzano Maldonado
José L. Jiménez Marquez
Carlos A. López Martínez
Gustavo García Pérez
Traslado de la cámara al lugar de la simulación del video
Colocación de extensión para alimentación eléctrica
Traslado de cartel para obstruir cámara de seguridad
Traslado de esferas para simulación de video
Obstrucción de la cámara de seguridad con cartel

Results:

- ✓ The fraud and the modus operandi to simulate the lottery results were detected.
- ✓ Computer forensics analysis helped to get stronger evidence against the public servants, in order to impose administrative and financial penalties.
- ✓ By the other hand, preliminary inquiry was strengthened through computers

forensics analysis and criminal actions were prosecuted by the corresponding judicial authorities.

- ✓ As it was said before, with the findings obtained from the computer forensics analysis it found sufficient evidence for the judicial authority to determine the impound of bank accounts, in which were deposited the economic resources that were fraudulently obtained, up to an amount of $ 110,000,000 million MXN.

B. Single types of digital evidence

1. Hash Values

The hash value is the result of a mathematical algorithm performed against a file or a hard drive. It is a unique digital thumbprint of the file or the hard drive as it exists at the time of the hashing process. There exist two types of hashes, MD5 and SHA1, both serving the same functions:

Hash value functions in digital forensic:
To verify that a forensic image of digital evidence is exactly the same of the original
To find hidden files in a computer, when the hash value of the original file is known
To determine whether a file with a known hash value exists on a computer

2. Metadata

Metadata is stored information about another data. It can be very useful for investigators, since it allows them to know a variety of information about a file, such as authorship, editing time, the machine on which the file was created.

Metadata is usually stored in:
Electronic Document
Picture
Webpage
Browser
File system

3. E-mail

Nowadays, e-mail is one of the most abundant forms of evidence available for investigators. This is essentially due to a series of factors: (i) most people use e-mail informally and candidly; (ii) many people believe that e-mail messages are impermanent; (iii) e-mails are more difficult to get rid of than most users believe, because of the ease of copying and forwarding, the fact that most e-mail systems require a two-step process to permanently delete e-mail from a system, and that the undeleted e-mails may be captured on system backups.[92]

E-mail is defined as a «document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the messages.»[93]

Information that can be retrieved
Content of the e-mail
Identification of the sender
Location of the sender
Identification of the consignee

Emails can be stored in multiple and different places, depending on the type of account, providing multiple opportunities for investigators to recover email even when they have been someway deleted.[94]

Email Servers
Corporate e-mail accounts They are typically hosted on a mail server, such Microsoft Exchange or Lotus Notes. These mail servers are usually backed up on a regular basis on tape or disk, while additional backups may be available at remote locations via off-site storage applications.
Free e-mail accounts Are hosted by companies who are in the business of marketing via the Internet. Today the biggest providers are Google Mail, Yahoo Mail and Microsoft Hotmail, even though many other free e-mail account providers are available to the public.
Internet Service Providers (ISPs) Provide e-mail accounts as part of the service when customers sign up for an account. These range from local ISPs who provide dial-up services in rural areas to high-speed

Internet providers via DSL, cable, or satellite.

Note: It is possible to get email messages from email internet providers via search warrant. Even though it varies by service providers, usually emails deleted by users are purged from the provider servers on a regular basis.

Personal Devices

Computers

Emails are stored in different formats trough several software that might be installed on the computer, such as Microsoft Outlook (file .pst), Outlook express (file .dbx), Apple mail (file .mbox). Even the use of a browser to navigate web –based mail account allows investigators to recover the emails that are cached on the hard drive as web pages.

*Cell Phones**,** Tablets and Pad Computers*

The operating system of portable devices provides for email client programs which makes readable email that are stored in the memory of the device.

Table 21: Best practices

The United States Experience - Challenges Associated with Obtaining and Utilizing the Content of Electronic Mail

SOURCE: The United States presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

How does this help in financial investigations?

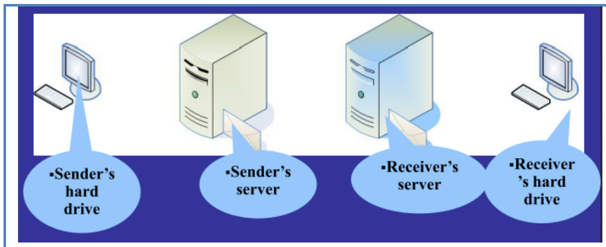
- Subject may have bank statements sent to their email address.
- Subject may be directing the movement of criminal proceeds by email.
- Communication between facilitators, and money launderers.

ECPA and Email

- Electronic Communications Privacy Act limits the United States' ability to obtain email evidence.

Where is someone's e-mail?

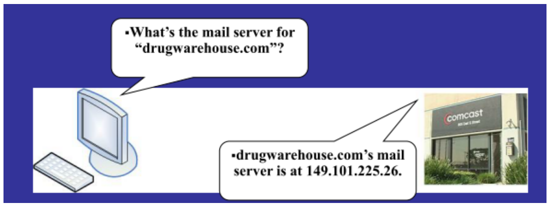
- Four copies, in different places
- Usually search the receiver's server



What do we search?

Where is their server?

- Domain name system


▪What's the mail server for "drugwarehouse.com"?
▪drugwarehouse.com's mail server is at 149.101.225.26.
comcast

Content available by search warrant

- To/From
- Attachments
- Subject Line
- Content of Messages
- IP Addresses

4. Cell phones and Cellular Systems

The usage of cell phones by suspects may allow investigators to retrieve a variety of information and potential forms of evidence, such as:

Data stored on the phone
Text messages, contact list, call history, pictures and any other type of document can be stored on cellphones. There exist three forensic methods to retrieve them:
▪ Physical acquisition: performed using a forensic software, is the best option since it allows to get all the types of data. It is not always possible.
▪ Logical acquisition: also performed using a forensic software, it is the second option since do not allow to recover every type of data.
▪ Manual acquisition: performed by an examiner who navigates the cell phone while takes picture of the screen, it is the last option when previous seen methods are not available.

Call detail records
Cellular service providers use derived information in call detail records for use in their

billing, coverage and analytics, such as:

- The date the call was made or received
- The time the call was made or received
- The number called/calling
- Usage type(voice, data, SMS, MMS)

Cell phone location

Even though a cell phone record cannot exactly locate the phone, it is possible to place the phone within a general area, corresponding to the radius of coverage of the cell tower that was connected to the phone in a specific moment.

5. Accounting software

Individuals and business use accounting programs, i.e. a software designed to manage the financial resources and to keep track of the money.

Personal accounting software

Allows individuals to manage personal money and home finances. These programs can reveal a lot of useful information about financial habits of the user. Since they can synchronize with the person bank, these type of programs allow investigators to retrieve bank accounts' information without ask for them to bank.

Business accounting software

Small, medium and multinational companies make use of accounting software to manage the money and to keep an audit trail that can be used to store information about every transaction.

c. Digital Forensic Tools

The following is a list of useful forensic tools[95]:

Forensic Suites (multiple tasks: acquisition, verification, analysis, preservation)

- EnCase (Guidance Software Corporation)
- FTK Forensic Tool Kit (Access Data Corporation)
- iLook LEO and iLookPI (Perlustro Corporation)
- SMART (ASR Data, Data Acquisition and Analysis, LLC)
- P2 Commander (Paraben Corporation)
- X-Ways Forensics (X-Ways Software Technology AG)
- MacForensicsLab (MacForensicsLab, Inc.)

- BlackLight Mac Analysis (BlackBag Technologies)

Acquisition Software

- EnCase Forensic Software (Guidance Software Corporation)
- Linen (Guidance Software Corporation)
- FTK Imager (Access Data Corporation)
- Forensic Replicator (Paraben Corporation)
- MacQuisition (BlackBag Technologies)
- Helix (e-fense)

Acquisition hardware devices

- Tableau
- Logicube
- Weibetech
- Intelligent Computer Solutions
- Voom Technologies

E-mail

- Email Examiner and Network Email Examiner (Paraben Corporation)
- Email Detective (Hot Pepper Technology)
- Mail Analyzer (Belkasoft)

Chat Programs

- Forensic software designed to recover chat logs from chat services such as Skype and others.
- Forensic IM Analyzer (Belkasoft)
- Chat Examiner (Paraben Corporation)

Internet History

- NetAnalysis (Digital Detective)
- Browser Analyzer (Belkasoft)

Mobile device

- Paraben Device Seizure (Paraben Corporation)
- Cellebrite (Cellebrite USA Corporation)
- Susteen SecureView (Susteen Inc.)
- CellDEK (Logicube)
- Mobilyze (BlackBag Technologies)
- BitPim (Open source free application)
- XRY (Micro Sysemation AB)
- Berla Corp GPS Forensic Software (Berla Corporation)

CHAPTER V. HUMAN INTELLIGENCE

People are a rich source of information in any investigation, since the very object of investigations is always the human behavior. This is the reason why intelligence derived from information collected and provided by human sources is essential in every class of investigation, and why, even in the digital era, human intelligence sources remain one of the key operational tools for law enforcement agencies.

A. Suspect profiling

When planning an investigation into a possible criminal conduct committed by an individual or a corporation, it is essential to identify the key information – and the related key questions –that are needed to set the ground for a deeper comprehension of the alleged facts and the suspect's profile, as well as to further develop the case.

Identifying key questions and target information is critical in order to establish a priority order among the sources of information to be consulted and the investigative actions to be taken. This also allows channeling the limited resources only to those selected leads which may result in the development of the most significant evidence in a timely manner.

Basic information can be organized into six categories, corresponding to six key questions about the alleged facts under investigation.[96]

Who?	
☐	Full name, plus any other identifying personal particulars, such as date of birth, current address, aliases, nicknames
☐	Criminal records reference number, or other adverse records, including previous intelligence traces
☐	Nationality, ethnicity, immigration status, language(s) and dialect(s)
☐	Family members, and the extent of their involvement

What?	
☐	Main criminal activities, other criminal activities
☐	Scale and frequency of criminal activities
☐	Nature of involvement, role
☐	Associates and contacts, including the nature of the relationships- 'Legitimate' business activities

Where?

- □ Main locations of criminal activities, plus reach (‘turf’) or spread
- □ Use of vehicles and other means of transport, including driving licence details and vehicle registration numbers
- □ Travel details, including passport details, routes

When?

- □ Actual dates, times
- □ Periods (from/to)

How?

- □ Criminal methods (how the business is organized and conducted)
- □ Means of communication, including telephone numbers, Internet use, use of coded language
- □ Assets employed (e.g., premises, vehicles, personnel)

Why?

- □ Rationale for particular actions and choices
- □ Motivation
- □ Attitudes (e.g., towards risk, criminal opportunities)
- □ Lifestyle (use of criminal profits to fund property purchases, vehicles, ‘nesteggs’, family support, entertainment, holidays, etc.)

When dealing with suspects of corruption, investigators should focus on those elements that have proven to be common in the stipulation and execution of a corrupt agreement.

The Briber: Private individual or entity

- □ All official data on the company: Trade Register; Stock Exchange
- □ Organizational charts for an adequate period of time, in particular:
- □ Location of the sales/marketing department
- □ Job descriptions, liabilities and executive powers in the company during the relevant time and in the relevant area
- □ Data on money flaws through bank account inquires
- □ Information on sales agreements
- □ Compare those data with similar companies’ data (business analysis)
- □ Expanses recorded in the nominal ledger
- □ Performances of sales and marketing staff:
- □ To whom they have sent invitations?
- □ What kind of hotel bills, parking tickets, lunch receipts, fight tickets or bus tickets

have been entered in the accounts? (this information can provide important insights about people involved)

□ Cross checking the receipts with agents' and other suspects' receipts might provide good evidence

□ Use of third party agents

□ Has the agency-.relationship been registered?

□ Where is the agent established?

□ Where, how and how much has he been paid?

□ How have those payments been recorded?

The Bribed: Public official

□ Public official income

□ Wealth disclosure statement

□ Job, income, wealth and other financial information about his family members

□ Place of residence

□ Activity of his office

□ Family house ownership and acquisitions

□ Cash flow analysis

□ University tuition of familiars

□ Vehicle ownership

□ Travels

□ Real estate ownership

□ Employment of family members

□ Academic tuition for family members

The investigators should be able to prioritize leads and information which may conduct to the development of a strong set of evidence against the offenders, for example:[97]

Personal residence

The personal residence ownership and acquisition transaction can reveal important information about the financial situation of the public official. A significant difference among the value of the purchase and the actual bank loan can reveal a very large initial payment at the time of purchase. Financial information relating to the purchase may be fairly easy to obtain in case the house had been purchased through a licensed Notary Public and the loan obtained at a major bank. The bank may maintain detailed records of the transaction, since they financed a significant amount and should have conducted due diligence which may have included the source of the initial payment. The Notary Public may also have records of the complete transaction. In some countries, it is customary to use 'title companies' or 'closing agents' that act as an escrow agent or middleman to facilitate the purchase of the property between the buyer and seller. These entities also maintain complete records of all money flows between the buyers, sellers, taxing authorities and financial institutions. The seller of the property should also be interviewed to obtain the complete details of the transaction, including the method of payment for the house.

Cash flow analysis

If the public official maintains a bank account at a domestic financial institution, the records of this account should be requested very early in the investigation because it may require a significant amount of time for the bank to research the records. If the government salary of the public official has been deposited into this domestic account, it will be important to perform a complete analysis to establish how his legitimate salary has been spent. A cash flow analysis relating to any cash withdrawals or deposits should also be prepared. Once these financial flows have been analyzed, it will create a complete picture of the distribution of his legal funds and show how much cash was available for purchases. This may be very significant if expenditures are later identified from unknown or illegal funds. Large cash payments or purchases from unknown sources may be an important piece of evidence at trial.

University education

A common way to reward a corrupted official has proven to be the coverage of college and university tuition for sons and other relatives of the public official. Investigations into the public official's family members may reveal, for example, that his sons are attending prestigious university abroad and there is a very good chance that the official is not able to afford the corresponding tuition, living expenses and travel costs. In this case, investigators should try to determine whether or not a legitimate source of funding, such as a scholarships granted by the university, exists, and who is actually paying the university tuitions. The universities should therefore be contacted, the expenditures documented and the source of payments identified.

Vehicle ownership

Another major lead from the pre-investigation activities might be vehicle ownership of the public official or of his family members. For example, the fact that the public official's wife owns an expensive automobile is an indication that he may be living above his means. Investigation into the purchase of the vehicle purchase will involve first tracing the ownership of the car to determine the prior owner. This can lead to discover the records of the transaction, who was the purchaser, the date of the purchase, and – the most important – the source of the payment. If the payment were made by bank check, the dealership may have a copy of it. If the payment was made by cash, this is a an interesting piece of evidence, provided for example that the cash analysis of the public official's bank account has established that he did not had available a corresponding amount of cash from his legitimate sources of income.

B. Informants and suspects

For investigations into corruption cases, human intelligence resources are particularly invaluable in circumstances where there is a real lack of information about the corrupt network. In the case of serious economic offences and corruption, the individual who comes forward may well be a disgruntled former employee, a whistleblower, a company representative who has been cheated out of a procurement deal by large-scale bribery or even a former co-conspirator with an axe to grind.[98]

However, investigators must pay careful attention to the reliability of these sources of information, by considering the reasons and the motives for the individual wishing to pass on information and whether those motives might be malicious, and therefore misleading, with the potential to compromise the investigation, and whether any sort of inducement is sought for the information.[99] Investigators should therefore seek to corroborate the information provided by informants through other sources of evidence and investigative tools.

When dealing with informants and witnesses, a comprehensive interviewing strategy should be developed. The following areas should be addressed:[100]

Informants and witnesses

□ Provisions should be in place for the protection of witnesses. Witnesses' identity should remain confidential for as long as possible. Witness relocation or protection programs or a "new identity" program may be available. If the witness is in prison, provisions for a safe location in must be established. The appropriate policies need to be developed as soon as possible so as to be in place when the need arises.

□ It is advisable to reduce opportunities for the defense lawyer to attack the credibility of the witnesses (by having recorded statements, transcribed and signed or initialed by the witness).

□ Processes should be established to deal with lawyers who are either attached to the witnesses or to the potential defendants.

□ If the witness has a criminal background, it is important that they be open about prior criminal activity (particularly if it involves the defendants) and to ensure sure that this information is disclosed to the court prior to the witness undergoing examination.

□ Keeping witnesses informed of the criminal prosecution process will instill confidence in them and allay fear and apprehension.

Specific considerations are to be made with reference to the different categories of informant and to specific needs.[101]

Confidential informants

They are generally criminals. Unlike a cooperating witness, their personal information must be maintained as confidential. The motives of the informant may be revenge, financial gain, or personal protection (i.e., to avoid being sentenced to prison). It is important to note that confidential informants are almost never expected to testify in court.

Confidential sources

They are generally not criminals, but they provide information because of their position or employment. Attention must be given to safeguarding these sources' income in order to prevent it from being jeopardized due to interaction with investigators.

Cooperating witnesses

Cooperating witnesses supply their information in a confidential manner, but they are expected to become witnesses. Remember the importance of protecting witnesses. When using a source or witness, as described above, internal protocols and procedures need to be established as uniform policy. The following elements are important:

□ Written agreements used to define the responsibilities of both the source and the law enforcement agency

□ A system of either code words or names established that will be used in files to prevent accidental disclosure

□ Original information kept separately from the general investigation files

□ Limited access to the source files for those within the investigative agency

□ Routinely audited financial records associated with source operations

□ A third party present when payments are made to a source and receipts obtained

□ Periodic reviews, at a managerial level, of the source files as an internal audit protection

□ Any promises being made to the informant or witness cleared with the government agency or government attorney (It is good policy to have all promises in writing to protect the integrity of the investigator and the investigative process)

Protection of the Source/Witness

Threats to the source or witness should be anticipated before they actually occur, and the investigative team should be prepared to immediately respond. A threat assessment should always be performed for witnesses, and it must always be determined if the witness is fearful of an approach or an act against their person. There are two approaches to threats to witnesses:

□ A reactive approach is the aggressive investigation of any threat or act of violence to a source. During this approach, no intimidation of any witness is tolerated

□ A proactive approach involves having witness assistance and witness protection programs available. It is important to remember that most witnesses are frightened simply by being involved in a criminal process. These concerns need to be dealt with by the team

Table 22: *Physiological stressors*

SOURCE: D. D. DORRELL - G. A. GADAWSKI - H. BOWEN - J. F. HUNT, Financial Intelligence: People and Money Techniques to Prosecute Fraud, Corruption, and Earnings Manipulation, in *The United States Attorney Bulletin,* March 2012, v 60, n. 2.

For the purpose of extract information from people and to be able to read the signals hidden into the complex and dynamic nature of the people, law enforcement agencies should rely on a series of techniques and tools, which analyze physiological stressors in order to evaluate a personal statement or examination.

Those techniques rely on the assumption that s*tress typically results when subjects fabricate responses to questions*, and that learning how to detect physical signs of stress reaction can therefore help investigators to realize whether or not a person under interrogation is lying.

The US Department of Justice makes reference to a variety of technique and methods, designed to comprehensively evaluate the physiological indicators of stress.

- The CICO method (Concentric-In/Concentric-Out), a comprehensive investigation/cross-examination technique, which comprises virtually all indicators affecting a subject and permits the assessment of the integrity, probity, or veracity of a subject's behavior, and oral or written statements.
- Dr. Paul Ekman tools, like FACS, F.A.C.E, METT, and SETT, specifically intended to interpreting facial expressions (www.paulekman.com);
- Don Rabon interrogation techniques, which make use of questions focused on auditory, visual, and sensory memory and recollection, and that stress that eye movement prior to answering a question indicates fabrication depending on the direction of the movement (www.hamletsmind.com);
- The Reid Technique of Interviewing® and Interrogation, developed by John Reid, widely deployed as a means of structuring interrogation leading to confession (www.reid.com);
- Linguistic Style Analysis Techniques (LSAT), deployed by Loveland Colorado Police Department, which consists of parsing verbal content into structural components in order to compare and contrast the facts (linguisticstatementanalysis.com);
- The Wicklander-Zulawski company methods of interrogation, lie detection, behavior detection (www.w-z.com).

References

[1] Further information regarding this workshop, including the agenda and presentations are available at http://www.fiscaliadechile.cl/apecactworkshopchile/index.html

[2] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 44, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[3] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 8

[4] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 29

[5] USAID Nepal, *Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case*, August 2005, p. 7-8, available at http://pdf.usaid.gov/pdf_docs/PNADE146.pdf. The gathering of evidence will be treated with more detail in the following Sections.

[6] *Reactive detection* takes place where a formal complaint –either from individuals, governmental agencies, or private companies, among others– is received by the law enforcement agency, forming the basis for investigation. Where the complaint comes from a governmental agency, it may be based on information derived from disclosure and reporting requirements as well as audits and inspections. Instead of complaint-based, *pro-active detection* is intelligence-based. It takes place, e.g., after law enforcement agencies conducted an undercover investigation pursuing intelligence information.

[7] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 36-38, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[8] For instance, when during the course of an integrity test the corrupt tendencies of an official may have been established, meaning that no further investigation is necessary.

[9] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 38, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[10] Ibid.

[11] UNODC, The Global Programme Against Corruption: UN Anti-Corruption Toolkit, 3nd Edition, Vienna, September 2004

[12] Recommendation Rec(2005)10 of the Committee of Ministers of the Council of Europe to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism.

[13] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 26-27, OECD, *Investigation and Prosecution of Corruption Offences: Materials for the Training Course*, Ukraine, 2012, p. 23-24

[14] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 11; UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 54, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[15] http://www.egmontgroup.org/about/financial-intelligence-units-fius.

[16] Conf. FATF Recommendation 31, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[17] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 22

[18] Article 48 of the UNCAC encourages law enforcement authorities in different jurisdictions to strengthen their co-operation in order to enhance the effectiveness of law enforcement action to combat corruption, through for example, the exchange of information and co-ordination of administrative actions for the purpose of early identification of the offence, as well as exchange of personnel and liaison officers.

[19] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations*, February 2012, Recommendation 32, p. 25, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[20] STAR (Stolen Asset Recovery) Initiative, The World Bank, UNODC, Barriers to Asset Recovery, Washington DC., 2011, p. 43, at http://www.unodc.org/unodc/en/corruption/StAR.html.

[21] FATF paper, best practices on confiscation (FATF 2010), available at: http://www.coe.int/t/dghl/monitoring/moneyval/web_ressources/FATF_BPR3&38.pdf

[22] Informal Expert Working Group on Effective Extradition Casework Best Practice (UNODC), Report. Vienna, 2004, p. 12, at http://www.unodc.org/documents/legal-tools/lap_report_ewg_extradition_casework.pdf.

[23] See *infra*.

[24] UNODC (United Nations Office on Drugs and Crime), Manual on Mutual Legal Assistance and Extradition, New York, 2012, p. 68, at http://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf.

[25] It is increasingly recognized that joint investigation teams (JITs) is an effective form of international co-operation in investigation and prosecution of trans-border corruption cases involving several countries.

[26] All APEC economies except for Hong Kong and Chinese Taipei are members of Interpol.

[27] See, http://www.interpol.int/About-INTERPOL/Overview.

[28] See, http://www.egmontgroup.org/.

[29] The FIUs of the following APEC economies are members of the Egmont Group: Australia, Canada, Chile, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand and The United States.

[30] ACPO, *Practice Advice On Financial Investigation*, p. 28.

[31] The process is based on the model developed in *ACPO (2005) Practice Advice on Core Investigative Doctrine*

[32] FATF, *Operational Issues. Financial Investigation Guidance*, p. 17.

[33] FATF, *Operational Issues. Financial Investigation Guidance*, p. 17.

[34] See www.cicad.oas.org/Lavado_Activos/ENG/Documents/Information%20Sources%20Exchange_Eng.doc.

[35] Association of Chief Police Officers (ACPO), *Practice Advice On Financial Investigation*, 2006

[36] US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Intelligence Community Directive*, Number 301. National Open Source Enterprise. Section F(3), July 11, 2006.

[37] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[38] US GAO, *Investigators' Guide to Sources of Information*, OSI-97-2, Apr 1, 1997, at www.gao.gov/products/OSI-97-2

[39] U.S. GAO*, SOCIAL MEDIA. Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, June 28, 2011, at www.gao.gov/products/GAO-11-605

[40] U.S. GAO*, SOCIAL MEDIA. Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, 2011.

[41] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 283.

[42] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 283.

[43] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.290.

[44] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.290.

[45] H.MULUKUTLA – M. RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, in INTERNATIONAL CENTRE FOR ASSET RECOVERY, *Tracing Stolen Assets: A Practitioner's Handbook*, Basel Institute on Governance, Basel, 2009, p. 79

[46] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46. See National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. Washington, DC: U.S. Government Printing Office, 413.

[47] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46.

[48] See D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.285.

[49] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46.

[50] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 47.

[51] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 47.

[52] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 291.

[53] M. K. Bergman, "The Deep Web: Surfacing Hidden Value", cited by David Hunter & Karen Brown, T*hriving or Surviving*? National Library of Scotland in 2030, National Library of Scotland, 2010, pp. 39/40.

[54] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 303.

[55] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 303.

[56] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 293.

[57] IACP NATIONAL LAW ENFORCEMENT POLICY CENTER, *Social Media, Concepts and Issues Paper*, September 2010, at www.iacpsocialmedia.org/Portals/1/documents/social%20media%20paper.pdf; INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, *Social Media Fact Sheet,* 2013, at www.iacpsocialmedia.org/Portals/1/documents/Fact%20Sheets/Social%20Media%20Fact%20Sheet.pdf

[58] COPS, *Social Media and Tactical Considerations For Law Enforcement*, May 2013, at www.iacpsocialmedia.org/Portals/1/documents/External/SocialMediaandTacticalConsiderationsforLawEnforcement.pdf

[59] See IACP CENTER FOR SOCIAL MEDIA, *2011 Survey Results*, at www.iacpsocialmedia.org/Resources/Publications/2011SurveyResults.aspx.

[60] LEXISNEXIS RISK SOLUTIONS, *Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations*, 2012, at www.lexisnexis.com/investigations.

[61] IACP NATIONAL LAW ENFORCEMENT POLICY CENTER*, Social Media, Concepts and Issues Paper*, September 2010, p.1.

[62] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 290.

[63] INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, *Social Media Fact Sheet,* 2013.

[64] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[65] See *Facebook Newsroom* at newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[66] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[67] D. TERDIMAN, *Report: Twitter Hits Half a Billion Tweets a Day,* in *CNET.COM*, October 26, 2012, at news.cnet.com/8301-1023_3-57541566-93/report-twitter-hits-half-a-billion-tweets-a-day/.

[68] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[69] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[70] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[71] COPS, *Social Media and Tactical Considerations For Law Enforcement*, at www.iacpsocialmedia.org/Portals/1/documents/External/SocialMediaandTacticalConsiderationsforLawEnforcement.pdf

[72] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[73] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[74] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[75] U.S. v. Joshua Meregildo et al., 11 Cr. 576 (WHP), August 10, 2012, at www.x1discovery.com/download/US_v_Meregildo.pdf.

[76] In the US, see for example, US GAO, *Investigators' Guide to Sources of Information*, OSI-97-2, Apr 1, 1997

[77] Based on US DEPARTMENT OF JUSTICE, *Financial Investigations Checklist*, at www.justice.gov/criminal/afmls/pubs/pdf/fininvguide.pdf.

[78] L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom*, Waltham, 2012, p. 3.

[79] J. KRAUSE, *Discovery Channels*, ABA Journal, July 2002, p. 50.

[80] J. LARUE et al., *Trails from the Aether: Cyber-Evidence*, in 54.1 State Bar of Texas 33rd Annual Advanced Family Law Course 1, 1 (2007), at www.texasbarcle.com/Materials/Events/6367/110331_01.pdf.; quoting D. BISHOP and A. HOROWITZ, *Electronic Discovery*, *Advanced Business & Commercial Litigation Course*, State Bar of Texas 2001, p. 1.

[81] S. L. HARRINGTON, *Contemporary Issues in Cyberlaw: Collaborating With a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?*, in *William Mitchell Law Review*, 2011, 38, 353, quoting W. E. MOOZ, Jr., *Technology Tips for Reducing EDD Review Costs*, 24 Legal Tech News, no. 12, March 2007, 1.

[82] THE RADICATI GROUP, *Email Statistics Report*, *2013-2017 Executive Summary*, at www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

[83] L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals*, p. 3.

[84] MULUKUTLA – RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, p. 78.

[85] MULUKUTLA – RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, p. 78.

[86] S. L. HARRINGTON, *Contemporary Issues in Cyberlaw: Collaborating With a Digital Forensics Expert,* p. 355.

[87] The following boxes are an adaptation from DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 11 ff.

[88] NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, April 2008, Washington, p. vii.

[89] The presented protocols and procedures largely represent an adaptation of guidance published in NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, p. 15 ff.; DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 25 ff.; SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, *Best Practices for Computer Forensic 2013*, at https://www.swgde.org/documents/Current%20Documents/09-14-2013%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0.

[90] DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 28.

[91] NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, p. 21.

[92] See J. E. FELDMAN, *The Basics of Computer Forensics*, p. 20, in *The Practical Litigator*, March 2001, 17.

[93] S. D. NELSON - B. A. OLSON - J. W. SIMEK, *The Electronic Evidence and Discovery Handbook*, American Bar Association, 2006, p. 259. The definition is also contained in the US Code of Federal Regulations (§1234.2).

[94] See DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 240 ff.

[95] See DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 36.

[96] See the SOCA *National intelligence requirement for serious organised crime*, 2008-9, as cited in A. BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, in INTERNATIONAL CENTRE FOR ASSET RECOVERY, *Tracing Stolen Assets: A Practitioner's Handbook*, Basel Institute on Governance, Basel, 2009, p. 39-40.

[97] Examples are taken from LASICH, *The Investigative Process – a Practical Approach*, p. 56 ff.

[98] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 45.

[99] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 45.

[100] USAID, *Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case*, August 2005, at pdf.usaid.gov/pdf_docs/PNADE146.pdf

[101] USAID, *Anticorruption Investigation and Trial Guide*, p. 6 ff.

APEC Project: M SCE 01 12A-1

Produced by

Guillermo Jorge
Guillermo Jorge y Asociados
Edificio Palacio Alcorta, Martín Coronado 3256, Of. 216,
C1425CSD, Buenos Aires – Argentina

For
Asia Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#213-ES-03.1.