

Chapter 17

A COST-EFFECTIVE MODEL FOR DIGITAL FORENSIC INVESTIGATIONS

Richard Overill, Michael Kwan, Kam-Pui Chow, Pierre Lai and Frank Law

Abstract Because of the way computers operate, every discrete event potentially leaves a digital trace. These digital traces must be retrieved during a digital forensic investigation to prove or refute an alleged crime. Given resource constraints, it is not always feasible (or necessary) for law enforcement to retrieve all the related digital traces and to conduct comprehensive investigations. This paper attempts to address the issue by proposing a model for conducting swift, practical and cost-effective digital forensic investigations.

Keywords: Investigation model, Bayesian network

1. Introduction

A digital forensic investigation involves the application of a series of processes on digital evidence such as identification, preservation, analysis and presentation. During the analysis process, digital forensic investigators reconstruct events in order to evaluate the truth of the forensic hypotheses related to the crime or incident based on the digital traces that have been identified and retrieved [2]. Due to inherent technological complexities, the identification and retrieval of digital traces cover a variety of techniques such as cryptography, data carving and data reconstruction. Each technique has a different level of complexity and, therefore, a different resource cost (e.g., expertise, time and tools).

Unlike physical events that are continuous, digital events are discrete and occur in temporal sequence [3]. Because of the discrete nature, it is possible to quantify the retrieval costs of individual digital traces. However, in the absence of a suitable model for digital forensic investigations, most investigators attempt to conduct a comprehensive retrieval

of all related digital traces despite the substantial costs associated with retrieving all the traces.

A more effective technique is to focus only on the digital traces that can be extracted in a cost-effective manner. The reasons are that investigating different digital traces requires resources (e.g., expertise, time and tools) in different amounts, and that the traces found have different evidentiary weights with respect to proving a hypothesis. The limited resources available for an investigation renders exhaustive search approaches impractical [4]. Consequently, digital forensic investigators who endeavor to retrieve all the traces – especially those that are not sufficient to prove the hypotheses – waste valuable resources.

This paper describes a model for conducting swift, practical and cost-effective digital forensic investigations. The model considers the retrieval costs of digital traces and incorporates a permutation analysis.

2. Preliminaries

Using the collective experience and judgment of digital forensic investigators, it is possible to rank the relative costs of investigating each trace T_i ($i = 1 \dots m$). The relative costs may be estimated in terms of their resource requirements (person-hours, access to specialized equipment, etc.) using standard business accounting procedures. The relative costs can be ranked $T_1 \leq T_2 \leq \dots \leq T_m$ without any loss of generality. As a direct consequence of this ranking, the minimum cost path for the overall investigation is uniquely identified.

Our focus is on digital traces residing on a hard disk. If the seized computer has sufficient storage, all the digital traces can be retrieved. If all the traces T_i ($i = 1 \dots m$) are retrieved, the minimum cost path is the permutation $[T_1 T_2 \dots T_m]$. An example of a permutation path is shown in Figure 1.

The number of possible paths at each step is given by $m!$ This is a direct consequence of the fact that the problem of selecting the next available trace from an ordered permutation of m distinct traces is isomorphic to the problem of selecting the next object from a collection of m identical objects.

In order to save time and conserve resources, it is useful to determine early in an investigation whether or not the investigation should continue. This requires an estimation of the cumulative evidentiary weight associated with the investigation as $W = \sum_{i=1}^m w_i$, where the (scaled) relative fractional evidentiary weight w_i of each trace T_i is either assigned by an expert or, by default, is set to one. The weight assignment process has to be undertaken only once as a preprocessing step for each distinct

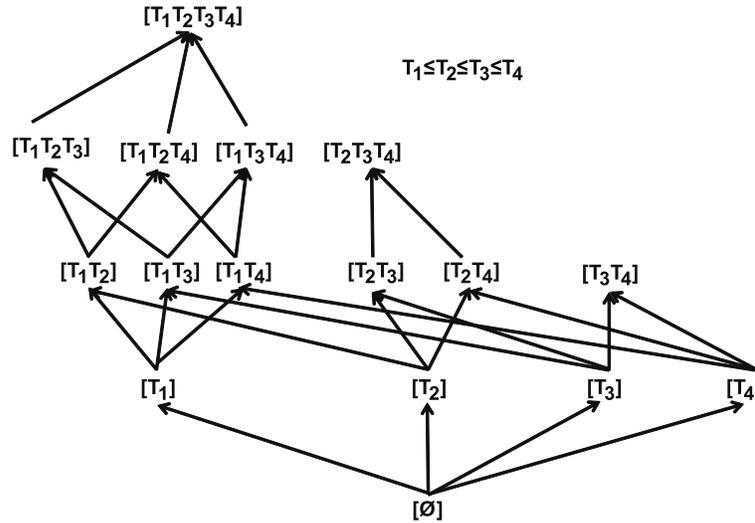


Figure 1. Path diagram with four traces.

digital crime template. If the cumulative estimate W is sufficiently close to one, the *prima facie* of the case can probably be established. Otherwise, it is unlikely that the available digital traces are sufficient to support the case.

The difference between W and one provides a “cut-off” condition that an investigator can use to avoid identifying all the traces exhaustively. The cut-off state is illustrated using the following example. Suppose that email exchanges between the culprit and victim are vital to an investigation. The forensic goal is to confirm that the computer, which was under the culprit’s control, had been used to send and receive the emails in question. Assume that the evidentiary traces are T_1, T_2, T_3, T_4, T_5 with evidentiary weights 0.05, 0.10, 0.15, 0.2, 0.35, respectively; and the evidentiary threshold is 0.85. Therefore, if all the traces are retrieved, then the estimated total evidentiary weight is 0.85, which indicates a strong case. On the other hand, if trace T_1 is not found, the overall evidentiary weight is 0.8, which is a 6% falloff. If both T_1 and T_2 are missing, the overall weight becomes 0.7, an 18% falloff. At this point, the forensic investigator should consider suspending the investigation as the prospect of successful prosecution is slim.

3. Missing Traces

Since a computer may not have sufficient storage, there is always the chance that some traces may be missing or overwritten. Thus, it may

not be possible for an investigator to ascertain all the trace evidence pertaining to a case. Suppose a certain trace T_j ($1 \leq j \leq m$) is not found. Then, all the investigative paths involving T_j are removed from the path diagram and the minimum cost path becomes $[T_1 T_2 \dots T_{j-1} T_{j+1} \dots T_m]$. The estimate of the evidentiary weight is $W = \sum_{i \neq j}^m w_i$.

Similarly, if two traces T_j and T_k ($1 \leq j; k \leq m; j \leq k$) are not found, then all the paths involving T_j or T_k must be deleted and the minimum cost path is $[T_1 T_2 \dots T_{j-1} T_{j+1} \dots T_{k-1} T_{k+1} \dots T_{m-1} T_m]$. The estimate of the evidentiary weight is $W = \sum_{i \neq j, k}^m w_i$. In general, if a total of k traces are not found ($1 \leq k < m$), then all the investigative paths containing any of the k traces must be deleted from the path diagram.

It is important to consider the issue of the independence of digital traces T_i . While the observations of the traces are necessarily independent because they are performed individually *post mortem*, the digital traces must be created independently if the model is to retain its validity. Since it is possible in principle for one user action to create multiple digital traces T_i (which are not mutually independent), care must be taken to ensure the independence of the expected digital traces when selecting the set of traces.

4. Investigation Model

The model for conducting cost-effective digital forensic investigations has two phases.

Phase 1 (Preprocessing – Detecting Traces)

- Enumerate the set of traces expected to be present based on the type of crime suspected.
- Assign relative investigation costs to each expected trace.
- Rank the expected traces in order of increasing relative investigation costs.
- Assign relative evidentiary weights w_i to each ranked trace.
- Rank the expected traces within each cost band in order of decreasing relative evidentiary weight.
- Set the cumulative evidentiary weight estimate W to zero.
- Set the total of the remaining available weights W_{rem} to one.
- For each expected trace taken in ranked order:
 - Search for the expected trace.
 - Subtract the relative evidentiary weight w_i of the trace from W_{rem} .

- If the expected trace is retrieved, add its relative evidentiary weight w_i to W .
- If W is sufficiently close to one, proceed to Phase 2.
- If $W + W_{rem}$ is not close enough to one, abandon the forensic investigation.

Phase 2 (Bayesian Network – Analyzing Traces)

- Run and analyze the Bayesian network model for the crime hypothesis using the retrieved traces as evidence (as described in [6]).

5. BitTorrent Case Study

This section uses a BitTorrent case study [6] to demonstrate the cost-effective digital forensic investigation model.

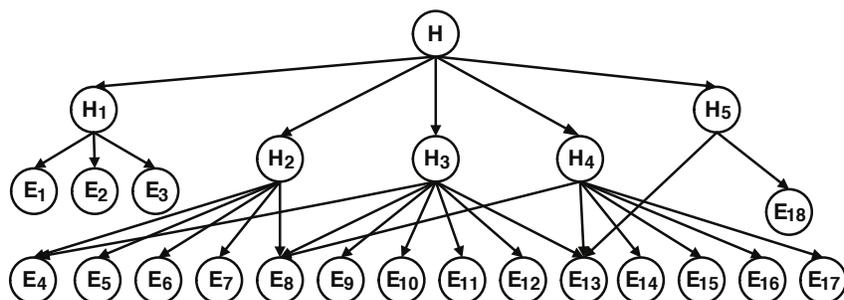
Figure 2 shows a Bayesian network with eighteen expected evidence traces (E_i) and their relationships to the five hypotheses (H_i). The Bayesian network is constructed by enumerating every path through which an evidentiary trace could have been produced and assigning it a probability.

The ideal case, in which all eighteen evidence traces are retrieved, is shown in Table 1. Note that each piece of trace evidence E_i is ranked according to its cost T_j .

The actual case, corresponding to a situation where two of the expected traces (E_8 and E_{14}) are missing, is shown in Table 2.

A potential complication involving the proposed investigation model should be noted. A trace could initially be assigned a low cost; however, upon further consideration, it could be determined that the cost is much higher. Examples of such a situation are a file that turns out to be protected by encryption or a partition that turns out to be deleted. In such cases, the cost of investigating the trace must be revised and all the traces must be ranked again based on the revised costs. This is necessary to maintain the minimum cost strategy for the investigation.

Constructing a Bayesian network model corresponding to an investigation requires the definition of the overall structure of the network, including the hierarchy of hypotheses and the associated posterior digital evidence (or traces) whose presence or absence determines the prior probabilities of the corresponding hypotheses. Next, numerical values are assigned to the prior probabilities. Traditionally, forensic investigators assign the prior probabilities based their expertise and experience.

**HYPOTHESES:**

- H** – The seized computer was used as the initial seeder to share the pirated file on a BitTorrent network
- H₁** – The pirated file was copied from the seized optical disk to the seized computer
- H₂** – A torrent file was created from the copied file
- H₃** – The torrent file was sent to newsgroups for publishing
- H₄** – The torrent file was activated and the computer connected to the tracker server
- H₅** – The connection between the seized computer and the tracker was maintained

EVIDENCE:

- E₁** – Modification time of the destination file is the same as that of the source file
- E₂** – Creation time of the destination file is after its modification time
- E₃** – Hash value of the destination file matches that of the source file
- E₄** – BitTorrent client software is installed on the computer
- E₅** – File link for the shared file is found
- E₆** – Shared file exists on the hard disk
- E₇** – Torrent file creation record is found
- E₈** – Torrent file exists on the hard disk
- E₉** – Peer connection information is found
- E₁₀** – Tracker server login record is found
- E₁₁** – Torrent file activation time is corroborated by its MAC time and link file
- E₁₂** – Internet history record of the publishing website is found
- E₁₃** – Internet connection is available
- E₁₄** – Cookie of the publishing website is found
- E₁₅** – URL of the publishing website is stored in the web browser
- E₁₆** – Web browser software is found
- E₁₇** – Internet cache record of the publishing of the torrent file is found
- E₁₈** – Internet history record of the tracker server connection is found

Figure 2. Bayesian network model for the BitTorrent case.

However, these assessments have been challenged in judicial proceedings primarily on the grounds that they are non-rigorous and subjective.

These challenges can be countered if a rigorous analytic procedure is used to quantitatively assign the prior probabilities. A promising

Table 1. Traces, relative costs and weights for the ideal BitTorrent case.

	Trace	Rel. Cost	Rel. Wt.	W	W_{rem}
	Initial Values			0	1
$T_1 (E_6)$	Shared file exists on the hard disk	1	2/18	2/18	16/18
$T_2 (E_1)$	Modification time of the destination file is the same as that of the source file	1	1/18	3/18	15/18
$T_3 (E_2)$	Creation time of the destination file is after its modification time	1	1/18	4/18	14/18
$T_4 (E_3)$	Hash value of the destination file matches that of the source file	1	1/18	5/18	13/18
$T_5 (E_8)$	Torrent file exists on the hard disk	1	1/18	6/18	12/18
$T_6 (E_{16})$	Web browser software is found	1	1/18	7/18	11/18
$T_7 (E_5)$	File link for the shared file is found	1	0.5/18	7.5/18	10.5/18
$T_8 (E_{15})$	URL of the publishing website is stored in the web browser	1	0.5/18	8/18	10/18
$T_9 (E_7)$	Torrent file creation record is found	1.5	2/18	10/18	8/18
$T_{10} (E_{13})$	Internet connection is available	1.5	2/18	12/18	6/18
$T_{11} (E_{10})$	Tracker server login record is found	1.5	0.5/18	12.5/18	5.5/18
$T_{12} (E_{12})$	Internet history record of the publishing website is found	1.5	0.5/18	13/18	5/18
$T_{13} (E_{14})$	Cookie of the publishing website is found	1.5	0.5/18	13.5/18	4.5/18
$T_{14} (E_{17})$	Internet cache record of the publishing of the torrent file is found	1.5	0.5/18	14/18	4/18
$T_{15} (E_{18})$	Internet history record of the tracker server connection is found	1.5	0.5/18	14.5/18	3.5/18
$T_{16} (E_4)$	BitTorrent client software is installed on the computer	2	2/18	16.5/18	1.5/18
$T_{17} (E_{11})$	Torrent file activation time is corroborated by its MAC time and link file	2	1/18	17.5/18	0.5/18
$T_{18} (E_9)$	Peer connection information is found	2	0.5/18	1	0

Table 2. Traces, relative costs and weights for the actual BitTorrent case.

	Trace	Rel. Cost	Rel. Wt.	W	W_{rem}
	Initial Values			0	1
$T_1 (E_6)$	Shared file exists on the hard disk	1	2/18	2/18	16/18
$T_2 (E_1)$	Modification time of the destination file is the same as that of the source file	1	1/18	3/18	15/18
$T_3 (E_2)$	Creation time of the destination file is after its modification time	1	1/18	4/18	14/18
$T_4 (E_3)$	Hash value of the destination file matches that of the source file	1	1/18	5/18	13/18
$T_5 (E_8)$	Torrent file exists on the hard disk (<i>missing</i>)	1	1/18	5/18	12/18
$T_6 (E_{16})$	Web browser software is found	1	1/18	6/18	11/18
$T_7 (E_5)$	File link for the shared file is found	1	0.5/18	6.5/18	10.5/18
$T_8 (E_{15})$	URL of the publishing website is stored in the web browser	1	0.5/18	7/18	10/18
$T_9 (E_7)$	Torrent file creation record is found	1.5	2/18	9/18	8/18
$T_{10} (E_{13})$	Internet connection is available	1.5	2/18	11/18	6/18
$T_{11} (E_{10})$	Tracker server login record is found	1.5	0.5/18	11.5/18	5.5/18
$T_{12} (E_{12})$	Internet history record of the publishing website is found	1.5	0.5/18	12/18	5/18
$T_{13} (E_{14})$	Cookie of the publishing website is found (<i>missing</i>)	1.5	0.5/18	12/18	4.5/18
$T_{14} (E_{17})$	Internet cache record of the publishing of the torrent file is found	1.5	0.5/18	12.5/18	4/18
$T_{15} (E_{18})$	Internet history record of the tracker server connection is found	1.5	0.5/18	13/18	3.5/18
$T_{16} (E_4)$	BitTorrent client software is installed on the computer	2	2/18	15/18	1.5/18
$T_{17} (E_{11})$	Torrent file activation time is corroborated by its MAC time and link file	2	1/18	16/18	0.5/18
$T_{18} (E_9)$	Peer connection information is found	2	0.5/18	16.5/18	0

approach is to use complexity theory [7]. Essentially, every path by which an evidential trace could have been produced is enumerated, and the probability associated with each path is evaluated using techniques from complexity theory.

We illustrate the approach using an example from the BitTorrent case. In particular, we evaluate the prior probability that hypothesis H_2 is true given that trace evidence E_8 (i.e., T_5) is found (Figure 2). E_8 is the evidence that the torrent file is present on the hard disk of the seized computer.

Three scenarios that result in the presence of the torrent file are:

- The file was placed on the seized computer by a covert malware process.
- The file was copied or downloaded to the seized computer from some other source.
- The file was created on the seized computer from the pirated file.

Assume that a state-of-the-art, anti-malware scan reveals the presence of a Trojan with a probability of approximately 0.98 [5]. Additionally, a thorough, careful inventory of the local networked drives and portable storage media reveals the presence of a source copy of the torrent file with a probability greater than 0.95. Furthermore, a high-quality search engine detects the presence of a downloadable copy of the torrent file with a similar probability [1]. As a result, the probability that the torrent file was created *in situ* on the hard disk of the seized computer is at least 0.88. The error bars for the assigned probabilities are derived assuming that the errors are normally distributed. Based on these assignments, we obtain a probability value of 0.94 ± 0.06 .

6. Conclusions

The proposed two-phase digital forensic investigation model achieves the twin goals of reliability and cost-effectiveness by incorporating a pre-processing phase, which runs in parallel with the data collection phase. The evidentiary weighting and cost ranking of the expected traces, which are undertaken only once for all similar investigations, enable the lowest cost traces to be examined first. This means that the “best-case” and “worst-case” scenarios can be processed efficiently. The combined use of evidentiary weights and ranked costs enables an ultimately futile investigation to be detected early and abandoned using only low cost traces. By the same token, an investigation that would ultimately prove to be unsuccessful could be halted before any high cost traces are investigated.

This model performs best in cases where the distributions of evidentiary weights versus costs are skewed towards low costs, and it performs the worst when the distributions are skewed towards high costs. In the average case, where the distribution is essentially unskewed (or even uniform), the model exhibits intermediate performance. However, it should be noted that, even in the most pathological cases, the performance would not be significantly worse than the current exhaustive or random search for traces.

One of the main advantages of the model is that it offers the possibility of creating templates of expected traces and their associated costs and evidentiary weights for every type of digital crime. These templates can provide investigators with benchmarks for calibrating their investigative procedures, and also offer novice investigators with an investigative model that can be adopted in its entirety.

References

- [1] S. Brin and L. Page, The anatomy of a large-scale hypertextual web search engine, *Computer Networks and ISDN Systems*, vol. 30(1-7), pp. 107–117, 1998.
- [2] B. Carrier and E. Spafford, Defining event reconstruction of digital crime scenes, *Journal of Forensic Sciences*, vol. 49(6), pp. 1291–1298, 2004.
- [3] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, London, United Kingdom, 2004.
- [4] Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights: Terrorism Bill and Related Matters, Third Report of Session 2005-06, HL Paper 75-I, HC 561-I, House of Lords, House of Commons, London, United Kingdom, 2005.
- [5] Kaspersky Lab, Free online virus scanner, Woburn, Massachusetts (www.kaspersky.com/virusscanner).
- [6] M. Kwan, K. Chow, F. Law and P. Lai, Reasoning about evidence using Bayesian networks, in *Advances in Digital Forensics IV*, I. Ray and S. Sheno (Eds.), Springer, Boston, Massachusetts, pp. 275–289, 2008.
- [7] S. Lloyd, Measures of complexity: A non-exhaustive list, *IEEE Control Systems*, vol. 21(4), pp. 7–8, 2001.

Chapter 18

ANALYSIS OF THE DIGITAL EVIDENCE PRESENTED IN THE YAHOO! CASE

Michael Kwan, Kam-Pui Chow, Pierre Lai, Frank Law and Hayson Tse

Abstract The “Yahoo! Case” led to considerable debate about whether or not an IP address is personal data as defined by the Personal Data (Privacy) Ordinance (Chapter 486) of the Laws of Hong Kong. This paper discusses the digital evidence presented in the Yahoo! Case and evaluates the impact of the IP address on the verdict in the case. A Bayesian network is used to quantify the evidentiary strengths of hypotheses in the case and to reason about the evidence. The results demonstrate that the evidence about the IP address was significant to obtaining a conviction in the case.

Keywords: Yahoo! Case, digital evidence, Bayesian network, reasoning

1. Introduction

Scientific conclusions based on evidence have been used for many years in forensic investigations. In making their assessments, investigators consider the available facts and the likelihood that they support or refute hypotheses related to a case. Investigators recognize that there is never absolute certainty and seek a degree of confidence with which to establish their hypotheses [2].

A forensic investigation determines the likelihood of a crime through the analysis and interpretation of evidence. To this end, a forensic investigation focuses on the validation of hypotheses based on the evidence and the evaluation of the likelihood that the hypotheses support legal arguments [6, 10, 12, 14, 15]. The likelihood represents the degree of belief in the truth of the associated hypothesis. It is typically expressed as a probability and probabilistic methods may be used to deduce the likelihood of a hypothesis based on the available evidence [7, 9].

A crime and its associated digital evidence are usually linked by sub-hypotheses. This paper uses a Bayesian network [8] to analyze and reason about the evidence in the well-known Yahoo! Case [3].

In the Yahoo! Case, Yahoo! Holdings (Hong Kong) Limited (Yahoo! HHKL) supplied IP address information to Chinese authorities that led to the conviction of Shi Tao, a Chinese journalist, for sending confidential state information to foreign entities. Shi Tao received a 10-year sentence for his crime.

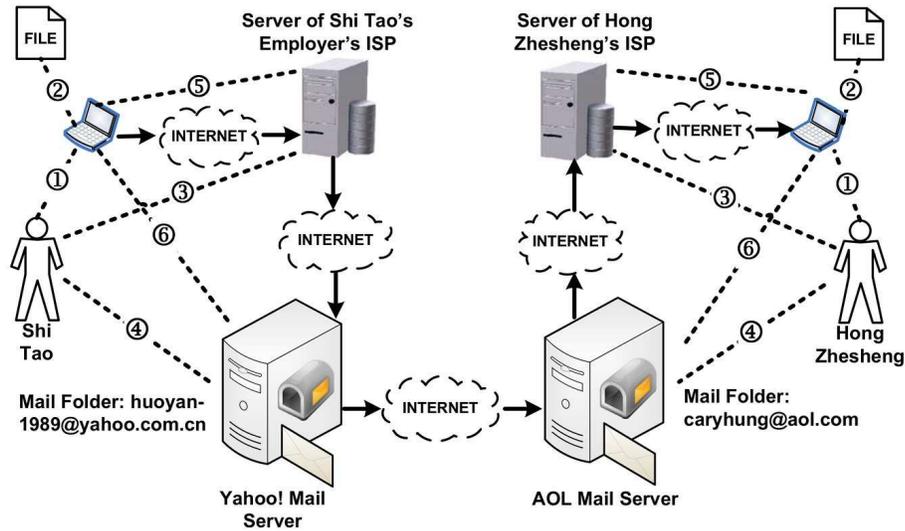
Shi Tao's authorized representative in Hong Kong subsequently lodged a complaint with the Office of the Privacy Commissioner for Personal Data. The complaint maintained that Yahoo! HHKL disclosed Shi Tao's "personal data" to Chinese authorities, which was a breach of the Hong Kong Personal Data (Privacy) Ordinance.

The investigation by the Privacy Commissioner concluded that an IP address, on its own, does not constitute personal data [13]. The conclusion was based on the position that an IP address is unique to a specific computer not a person and, therefore, does not meet the definition of personal data. The Privacy Commissioner also held that no safe conclusion could be drawn that user data corresponding to the IP address belonged to a living individual as opposed to a corporate or unincorporated body, or that it was related to a real as opposed to a fictitious individual.

We use Bayesian network inference to assess the evidentiary weight of the IP address in the Yahoo! Case. Four scenarios are evaluated:

- Yahoo! HHKL and the ISP participate in the investigation; all the digital evidence is available.
- Yahoo! HHKL participates in the investigation; digital evidence regarding the IP address is received from Yahoo! HHKL. However, the ISP does not participate in the investigation.
- Yahoo! HHKL does not participate in the investigation; digital evidence regarding the IP address is not received from Yahoo! HHKL. However, the ISP participates in the investigation.
- Yahoo! HHKL and the ISP do not participate in the investigation; no digital evidence regarding the IP address is available.

Although an IP address, by itself, is not viewed as personal data, our analysis shows that it carried significant evidentiary weight in the Yahoo! Case. Our analysis is based on the "Reasons for Conviction" [4], and the Administrative Appeals Board decision [1] regarding the Report of the Hong Kong Privacy Commissioner published under Section 48(2) of the Personal Data (Privacy) Ordinance (Chapter 486) [13].



- ① Shi Tao (Hong Zhesheng) controls the computer.
- ② The attached file exists on Shi Tao's (Hong Zhesheng's) computer.
- ③ Shi Tao's employer's (Hong Zhesheng's) ISP subscription record.
- ④ Shi Tao's (Hong Zhesheng's) Yahoo! (AOL) email account registration record.
- ⑤ The computer connects to the ISP.
- ⑥ The web browser program displays the Yahoo! (AOL) email web page.

Figure 1. Entities and events in the Yahoo! Case.

2. Digital Evidence in the Yahoo! Case

In the Yahoo! Case, the Changsha Intermediate People's Court of Hunan Province convicted Shi Tao of providing state secrets to foreign entities. Based on the data provided by Yahoo! HHKL, the court determined that at approximately 11:32 pm on April 20, 2004, Shi Tao used a computer in his employer's office to access his personal email account (huoyan-1989@yahoo.com.cn) via the Yahoo! webmail interface and send some notes regarding a summary of a top-secret document issued by the Chinese Government to the email account of Hong Zhesheng (caryhung@aol.com) [13]. Shi Tao asked Hong Zhesheng, who resided in New York, to find a way to distribute the notes as quickly as possible without using Shi Tao's name [5].

Figure 1 shows the entities and events involved in the email transmission from Shi Tao to Hong Zhesheng. Based on this description, a digital forensic investigator would be required to ascertain the following facts:

1. Shi Tao had access to a computer connected to the Internet.
2. A copy of the electronic file was stored on the computer.
3. The computer had a web browser program.
4. To obtain Internet access, Shi Tao established a connection between the computer and the ISP. In this case, he used the dial-up account belonging to his employer. The ISP authenticated the account of Shi Tao's employer and assigned an IP address to Shi Tao's computer. Shi Tao's computer recorded the assigned IP address and used it for subsequent Internet access. Internet data originating from or destined to Shi Tao's computer went through the ISP.
5. Shi Tao launched the web browser program and entered the Yahoo! webmail URL in the browser window.
6. The web browser program sent an HTTP request to the Yahoo! mail server. When the requested web page was retrieved, it was displayed by the web browser program.
7. Shi Tao entered his user name and password to log into his email account. Based on the email subscription details, the Yahoo! mail server authenticated Shi Tao and allowed him to log into his email folder.
8. Shi Tao composed the email, attached the file and entered Hong Zhesheng's AOL email address. He then clicked the "Send" button to transmit the email along with the file attachment. Since Shi Tao used a web browser program to create the email, the email content was (possibly) cached in Shi Tao's computer.
9. The Yahoo! email server stored the email and the attachment, and placed it in the message queue for transmission to Hong Zhesheng's AOL email server via SMTP.

3. Evaluation of Digital Evidence

In general, an investigation must clarify a number of issues before a case can be brought to court. These issues include whether or not a crime was committed, how the crime was committed, who committed the crime and whether or not there is a reasonable chance of conviction.

We use a Bayesian network to quantify the evidentiary strengths of hypotheses and to reason about evidence. A Bayesian network is a directed acyclic graph whose edges indicate dependencies between nodes.

Each node is accompanied by a conditional probability table (CPT) that describes the dependencies between nodes. In our work, the nodes correspond to hypotheses and the digital evidence associated with hypotheses. The edges connect each hypothesis to the evidence that should be present if the hypothesis is valid.

4. Bayesian Network

The first step in constructing a Bayesian network for analyzing digital evidence in the Yahoo! Case involves the definition of the primary hypothesis (H), the main issue to be determined. In the Yahoo! Case, the primary hypothesis is: “The seized computer was used to send the material document as an email attachment using a Yahoo! webmail account.”

The next step is to define the possible states of the hypothesis (Yes, No and Uncertain). Probability values are then assigned to each state. Each of these values represents the prior probability that the hypothesis is in the specific state. The prior probability of H , $P(H)$, is assumed to be equal to (0.333, 0.333, 0.333), i.e., all three states are equally likely.

The hypothesis H is the root node in the Bayesian network. Sub-hypotheses that are causally dependent on the hypothesis assist in proving the hypothesis. The sub-hypotheses and the associated evidence and events are represented as child nodes in the Bayesian network.

Figure 1 lists six sub-hypotheses that support the primary hypothesis H in the Yahoo! Case. The six sub-hypotheses are:

- H_1 : Linkage between the material document and the suspect’s computer (Table 1).
- H_2 : Linkage between the suspect and the computer (Table 2).
- H_3 : Linkage between the suspect and the ISP (Table 3).
- H_4 : Linkage between the suspect and the Yahoo! email account (Table 4).
- H_5 : Linkage between the computer and the ISP (Table 5).
- H_6 : Linkage between the computer and the Yahoo! email account (Table 6).

The evidence and events for the six sub-hypotheses are listed in Tables 1–6.

The states of the various sub-hypotheses are dependent on the state of H . Each sub-hypothesis, which is a child node of H , has an associated conditional probability table (CPT). The CPT contains the prior

Table 1. H_1 : Linkage between the material document and the suspect's computer.

ID	Evidence Description	Type
DE1	Subject file exists on the computer	Digital
DE2	Last access time of the subject file is after the IP address assignment time by the ISP	Digital
DE3	Last access time of the subject file matches or is close to the sent time of the Yahoo! email	Digital

Table 2. H_2 : Linkage between the suspect and the computer.

ID	Evidence Description	Type
PE1	Suspect was in physical possession of the computer	Physical
DE4	Files on the computer reveal the identity of the suspect	Digital

Table 3. H_3 : Linkage between the suspect and the ISP.

ID	Evidence Description	Type
DE5	ISP subscription details match the suspect's particulars	Digital

Table 4. H_4 : Linkage between the suspect and the Yahoo! email account.

ID	Evidence Description	Type
DE6	Subscription details of the Yahoo! email account match the suspect's particulars	Digital

Table 5. H_5 : Linkage between the computer and the ISP.

ID	Evidence Description	Type
DE7	Configuration settings for the ISP Internet account are found on the computer	Digital
DE8	Log data confirms that the computer was powered up at the time the email was sent	Digital
DE9	Web program or email user agent program was found to be activated at the time the email was sent	Digital
DE10	Log data reveals the assigned IP address and the assignment time by the ISP to the computer	Digital
DE11	Assignment of the IP address to the suspect's account is confirmed by the ISP	Digital

Table 6. H_6 : Linkage between the computer and the Yahoo! email account.

ID	Evidence Description	Type
DE12	Internet history logs reveal that the Yahoo! email account was accessed by the computer	Digital
DE13	Internet cache files reveal that the subject file was sent as an attachment via the Yahoo! email account	Digital
DE14	Yahoo! confirms the IP address of the Yahoo! email with the attached document	Digital

probabilities of the sub-hypothesis based on the state of the hypothesis. The probability values are typically assigned by digital forensic experts based on their subjective beliefs.

Table 7. Conditional probabilities of $H_1 \dots H_6$.

H	$H_1 \dots H_6$		
	Yes	No	Uncertain
Yes	0.60	0.35	0.05
No	0.35	0.60	0.05
Uncertain	0.05	0.05	0.90

We assume that all the sub-hypotheses ($H_1 \dots H_6$) have the CPT values shown in Table 7. For example, an initial value of 0.6 is assigned for the situation where H and H_1 are Yes. This means that when the seized computer was used to send the material document as an email attachment using a Yahoo! webmail account, the probability that a linkage existed between the material document and the seized computer is 0.6. Additionally, there may be instances where it is not possible to confirm a Yes or No state for H_1 from the evidence although the seized computer was used to send the document. This uncertainty is modeled by assigning a probability of 0.05 to the Uncertain state.

After assigning conditional probabilities to the sub-hypotheses, the observable evidence and events related to each sub-hypothesis are added to the Bayesian network. For reasons of space, we only discuss Hypothesis H_1 (Linkage between the material document and the seized computer) in detail to demonstrate the use of a Bayesian network.

The evidence for H_1 that establishes the linkage between the material document and the seized computer includes: (i) the subject file exists on the computer; (ii) the last access time of the subject file is after the IP address assignment time by the ISP; and (iii) the last access time of

Table 8. Conditional probabilities of E_1, E_2, E_3 .

H_1	E_1			E_2			E_3		
	Y	N	U	Y	N	U	Y	N	U
Y	0.85	0.15	0	0.85	0.15	0	0.85	0.12	0.03
N	0.15	0.85	0	0.15	0.85	0	0.12	0.85	0.03
U	0	0	1	0	0	1	0.03	0.03	0.94

the subject file matches or is close to the sent time of the Yahoo! email. Each node has the states: Yes (Y), No (N) and Uncertain (U).

The next step is to assign conditional probability values to the evidence. Table 8 shows the conditional probability values of evidence E_1 , E_2 and E_3 given specific states of Hypothesis H_1 .

After conditional probabilities are assigned to the entailing evidence, it is possible to propagate probabilities within the Bayesian network. In particular, the likelihood of H_1 is computed based on the observed probability values of evidence E_1 , E_2 and E_3 . The well-known MSBNX program [11] was used to propagate probabilities in the Bayesian network developed for the Yahoo! Case.

If evidence E_1 , E_2 and E_3 have Yes states, then the digital forensic investigator can confirm that there is a likelihood of 99.6% that Hypothesis H_1 (Linkage between the material document and the suspect's computer) is true. Furthermore, based on the 99.6% likelihood for H_1 , the investigator can also conclude that there is a 59.9% likelihood that H (The seized computer was used to send the material document as an email attachment using a Yahoo! webmail account) is true. Figure 2 shows the Bayesian network when E_1 , E_2 and E_3 all have Yes states.

The same methodology is used to compute the likelihoods of the other five sub-hypotheses based on the probability values of the associated evidentiary nodes. Finally, the likelihoods of the six sub-hypotheses are used to compute the overall likelihood of the primary hypothesis.

5. Impact of the IP Address

In order to assess the evidentiary weight of the IP address in the Yahoo! Case, we identify four scenarios that involve differing amounts of evidence provided to the Chinese authorities by Yahoo! HHKL and the ISP.

- **Scenario 1:** In this scenario, Yahoo! HHKL and the ISP participate in the investigation. When all the evidence (DE1–DE14

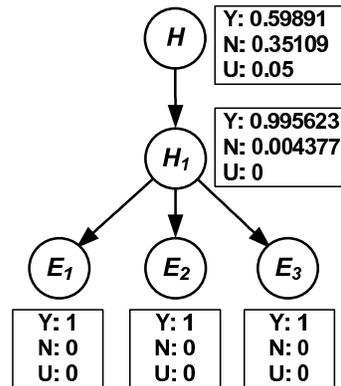


Figure 2. Probability distributions with $E_1, E_2, E_3 = \text{Yes}$.

and PE1) in Tables 1–6 is available and is true, the likelihood of Hypothesis H is 90.5%.

- **Scenario 2:** In this scenario, the ISP does not participate in the investigation. The evidentiary items DE5 (Table 3) and DE11 (Table 5) are missing. The corresponding likelihood of Hypothesis H is 88.1%.
- **Scenario 3:** In this scenario, Yahoo! HHKL does not participate in the investigation. The evidentiary items DE6 (Table 4) and DE14 (Table 6) are missing. The corresponding likelihood of Hypothesis H is 83.0%.
- **Scenario 4:** In this scenario, Yahoo! HHKL and the ISP do not participate in the investigation. Evidentiary items DE5 (Table 3), DE6 (Table 4), DE11 (Table 5) and DE14 (DE14) are missing. The corresponding likelihood of Hypothesis H is 78.7%.

Table 9 lists the four scenarios and their likelihoods. Note that the availability of the IP address affects the likelihood by 11.7%. In particular, the likelihood is 90.5% (very likely) when all the evidence is available, but it drops to 78.7% (probable) when evidence related to the IP address is not available. Although the IP address by itself does not reveal the identity of a specific user, it provides additional information that can further confirm the identity of the user.

The Reasons for Verdict [5] in the Yahoo! Case identified six primary facts:

- **Fact 1:** Shi Tao attended the press briefing and obtained the information.

Table 9. Likelihood of Hypothesis H .

Scenario	Likelihood
Scenario 1: Yahoo! HHKL and the ISP participate in the investigation	90.5%
Scenario 2: Yahoo! HHKL participates in the investigation and confirms the IP address of the Yahoo! email with the attached document; the ISP does not participate in the investigation	88.1%
Scenario 3: Yahoo! HHKL does not participate in the investigation; the ISP participates in the investigation	83.0%
Scenario 4: Yahoo! HHKL and the ISP do not participate in the investigation	78.7%

- **Fact 2:** Shi Tao was present in the office of his employer at the material time.
- **Fact 3:** Shi Tao was the only employee who knew the information.
- **Fact 4:** The office of the employer was the registration address for the IP address.
- **Fact 5:** The IP address was assigned to the employer at the time the email was sent.
- **Fact 6:** The email was sent from the material IP address.

We developed a Bayesian network modeling these facts to evaluate the hypothesis: “Shi Tao sent the material email at the material time from the office of his employer.” Experiments with the Bayesian network indicate that when all six facts are completely supported, the likelihood of Hypothesis H is 99.9%. However, when the IP address is missing (i.e., Facts 4–6 relating to the IP address are Uncertain), the overall likelihood drops to 14.9%, a reduction of 85.0%. This drop underscores the importance of the IP address in obtaining a conviction in the Yahoo! Case.

6. Conclusions

Bayesian networks provide a powerful mechanism for quantifying the evidentiary strengths of investigative hypotheses and reasoning about evidence. The application of a Bayesian network to analyze digital evidence related to the Yahoo! Case demonstrates that the IP address was significant to obtaining a conviction. Investigators and prosecutors can use this technique very effectively to evaluate the impact of specific evidentiary items before a case is brought to court.

References

- [1] Administrative Appeals Board, Shi Tao v. The Privacy Commissioner for Personal Data, Administrative Appeal No. 16 of 2007, Hong Kong (www.pcpd.org.hk/english/publications/files/Appeal_Yahoo.pdf), 2007.
- [2] C. Aitken and F. Taroni, *Statistics and the Evaluation of Evidence for Forensic Scientists*, John Wiley and Sons, New York, 2004.
- [3] R. Bascuas, Property and probable cause: The Fourth Amendment's principled protection of privacy, *Rutgers Law Review*, vol. 60(3), pp. 575–645, 2008.
- [4] Changsha Intermediate People's Court of Hunan Province, Criminal Verdict, First Trial Case No. 29, Changsha Intermediate Criminal Division One Court, Changsha, China (www.globalvoicesonline.org/wp-content/ShiTao_verdict.pdf), 2005.
- [5] Changsha Intermediate People's Court of Hunan Province, Reasons for Verdict, First Trial Case No. 29, Changsha Intermediate Criminal Division One Court, Changsha, China (www.pcpd.org.hk/english/publications/files/Yahoo_annex.pdf), 2005.
- [6] R. Cook, I. Evett, G. Jackson, P. Jones and J. Lambert, A model for case assessment and interpretation, *Science and Justice*, vol. 38, pp. 151–156, 1998.
- [7] P. Dawid, Statistics and the Law, Research Report No. 224, Department of Statistical Science, University College London, London, United Kingdom, 2004.
- [8] F. Jensen, *An Introduction to Bayesian Networks*, Springer-Verlag, New York, 1996.
- [9] M. Kwan, K. Chow, F. Law and P. Lai, Reasoning about evidence using Bayesian networks, in *Advances in Digital Forensics IV*, I. Ray and S. Sheno (Eds.), Springer, Boston, Massachusetts, pp. 275–289, 2008.
- [10] R. Loui, J. Norman, J. Altepeter, D. Pinkard, D. Craven, J. Lindsay and M. Foltz, Progress on Room 5: A testbed for public interactive semi-formal legal argumentation, *Proceedings of the Sixth International Conference on Artificial Intelligence and Law*, pp. 207–214, 1997.
- [11] Microsoft Research, MSBNx: Bayesian Network Editor and Tool Kit, Microsoft Corporation, Redmond, Washington (research.microsoft.com/adapt/MSBNx).

- [12] J. Mortera, A. Dawid and S. Lauritzen, Probabilistic expert systems for DNA mixture profiling, *Theoretical Population Biology*, vol. 63(3), pp. 191–206, 2003.
- [13] Office of the Privacy Commissioner for Personal Data, Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Chapter 486), Report No. R07-3619, Hong Kong (www.pcpd.org.hk/english/publications/files/Yahoo_e.pdf), 2007.
- [14] H. Prakken, C. Reed and D. Walton, Argumentation schemes and generalizations in reasoning about evidence, *Proceedings of the Ninth International Conference on Artificial Intelligence and Law*, pp. 32–41, 2003.
- [15] D. Walton, Argumentation and theory of evidence, in *New Trends in Criminal Investigation and Evidence – Volume II*, C. Breur, M. Kommer, J. Nijboer and J. Reijntjes (Eds.), Intersentia, Antwerp, Belgium, pp. 711–732, 2000.