Symmetry **2015**, *7*, 383-394; doi:10.3390/sym7020383

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

The Digital Fingerprinting Analysis Concerning *Google Calendar* under Ubiquitous Mobile Computing Era

Hai-Cheng Chu [1], Gai-Ge Wang [2] and Jong Hyuk Park [3,*]

[1] Department of International Business, National Taichung University of Education, 140 Min-Shen Road, Taichung 40306, Taiwan; E-Mail: hcchu@mail.ntcu.edu.tw

[2] School of Computer Science and Technology, Jiangsu Normal University, Xuzhou, Jiangsu 221116, China; E-Mail: gaigewang@163.com

[3] Department of Computer Science and Engineering, Seoul National University of Science and Technology, 172 Gongneung-dong 2, Nowon-gu 139743, Korea

* Author to whom correspondence should be addressed; E-Mail: parkjonghyuk1@hotmail.com; jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702; Fax: +82-2-977-9441.

Academic Editor: Laurence Yang

Received: 28 December 2014 / Accepted: 8 April 2015 / Published: 17 April 2015

Abstract: Internet Communication Technologies (ICTs) are making progress day by day, driven by the relentless need to utilize them for everything from leisure to business. This inevitable trend has dramatically changed contemporary digital behavior in all aspects. Undoubtedly, digital fingerprints will be at some point unwarily left on crime scenes creating digital information security incidents. On the other hand, corporates in the private sector or governments are on the edge of being exploited in terms of confidential digital information leakages. Some digital fingerprinting is volatile by its nature. Alternatively, once the power of computing devices is no longer sustainable, these digital traces could disappear forever. Due to the pervasive usage of *Google Calendar* and *Safari* browser among network communities, digital fingerprinting could be disclosed if forensics is carried out in a sound manner, which could be admitted in a court of law as probative evidences concerning certain cybercrime incidents.

Keywords: intangible digital traces; Google calendar; *Safari* browser forensics; volatile memory acquisition

1. Introduction

Evidently, the extensive usage of on-line *Google Calendar* and *Safari* assists global users in respect to working in groups or teams or for the purpose of achieving synchronization of pre-arranged itineraries. Millions of individuals benefit from the above on-line cooperative team working mechanisms in terms of arranging itineraries according to on-line calendars. This phenomenon has exponentially increased in recent years. Although *Google Calendar* has authorization processes for participants, information security and privacy concerns are still crucial factors to be considered. On the other hand, these digital records could be revealed in some way in order to provide probative evidences in a court of law for the purpose of judging a suspect to be innocent or culpable [1,2]. Under the current ubiquitous networking infrastructures, by means of Digital Forensics (DF) scientific approaches, the invisible, fragile, and intangible digital trails could be disclosed by way of appropriate systematic procedures.

Undoubtedly, the contemporary ICT has spawned various types of on-line information sharing Application Programs (APs). On-line cooperation across geographical limitation has allowed global individuals to arrange tentative schedules within the organizations in order to establish the connections with respect to certain common goals. This utilization poses new directions for the efficient and robust information sharing mechanisms among working communities to fulfill their business goals via heterogeneous mobile computing devices through ubiquitous networking systems [3–5]. Without loss of generality, the cybercrime syndicate may take advantage of these ICT APs to commit illegal conspiracies for the sinister and lucrative activities. The utilization of on-line *Google Calendar* is growing in an unprecedented pace and is becoming a preferable methodology for the working communities to synchronize the cooperative tasks in the digital era.

Obviously, the Random Access Memory (RAM) of any computing devices plays an essential role to store the temporary data and they are volatile in their natures. Substantively, by means of acquisition of the temporary data within the RAM, decisive digital traces could be revealed via systematic procedures. Once the power of the computing device is no longer sustainable, those digital trails will be gone forever [6–9].

The aim of this promising research is to collect, analyzed, synthesized, and present the related digital traces in *Google Calendar* with theory and practice. Nowadays, *Google Calendar* and *Safari* browser have become one the dominant tools for the distinct web communities to complete their daily tasks. Definitely, they also become one of the major the platforms for the cybercrime syndicate to commit illegal activities. In this research, we provide the generic methodologies as the references for the DF experts to ponder when similar situations occur.

The rest of the paper is organized as the followings. In Section 2, we present wide-ranging literature reviews, which have been discovered in the contemporary DF research field. In Section 3, we illustrate the design of the experiment in a step-by-step manner. In Section 4, we summarize and discuss the experiment results with respect to the digital traces that have been identified, collected, transported, preserved, analyzed, interpreted, cross-referenced, and presented in systematic procedures based on the proposed methodologies in this paper. At last, we provide the conclusions of this challenging research work in Section 5.

2. Literature Reviews

The rapid progress of ICT and the convergences of communications and computing have dramatically changed the way for contemporary global civilians. By the virtue of ubiquitous communication environments, voluminous tedious tasks could be fulfilled with only several touches on the mobile computing gadgets, which could be phenomenally impossible decades ago. Regrettably, the ICT savvy crime syndicates, which were not foreseeable before have become reality in our digital era [10–13]. The continuous application of digital technologies will pave the roads for providing innumerable and heinous cyber conspiracies in all aspects. In a nutshell, the digital platforms are providing an unparalleled avenue for the cyber criminals who are highly educated with sophisticated ICT training.

On-line cooperation and synchronization within the organizations in terms of collaborative tasks have become the current trend for team members to utilize without the limitations of the time zone issue, geographic concern, and heterogeneous types of computing devices. In parallel to the aforementioned significant growth, metamorphic data are interrelated due to the interactions among community users, especially in the modern social networking services arena [5,14–16]. Most web-based APs rely on suitable web browsers in order to fulfill the above goals. For example, *Safari*, *Google Chrome*, *Internet Explorer*, and *Firefox* are the popular ones.

Social networking activities stimulates the urge for the DF experts to focus because they contain quite a few unrevealed, hidden, decisive elements that are digitalized as the evidences to be admitted in a court of law. Some networking activities are executing via web browsers and there are varieties of ones in the current markets. Since the web browsers play an essential role for global users to surf the Internet, digital fingerprinting will be unwarily left associate with the browser being utilized. Consequently, the web browser forensics will be critical in terms of disclosing the digital traces via the extraction of significant, intangible, and critical information, which could be the probative evidences for criminal cases [17–20].

The prevalence of social networking activities generates uncountable and precious information such as service logs and service relationship [1,4,21]. This situation is hastily, phenomenally, and unknowingly occurring in an unparalleled pace in our digital societies. The appropriate procedures to create and manage invisible digital trails from the social networking web sites are imminent and indispensable for law enforcement agencies in the public sector. In private sector, some of aforementioned statements are close to the fraud of business related operations. However, through the systematic and appropriate approaches to deal with the digital fingerprinting discovery is another urgent task with respect to the mushrooming cybercrimes.

3. Design of the Experiment

Pre-Deployments of the Experiments

Phase 1: As Figure 1 indicates, the DF team deliberately marked two itineraries on 1 February 2013 as arrow #2 points in Figure 1 and 1 December 2013 as arrow #2 in Figure 2, respectively. The event being posted on the former itinerary between 6:00 a.m. and 7:00 a.m. was *AAFF1357* as arrow #3 points in Figure 1. It indicates that the user name was *ludy CHEN* as arrow #1 points in Figure 1. In addition, the item being posted on the latter itinerary between 6:00 p.m. and 7:00 p.m. was *BBEE2222* as arrow #3 points in Figure 2. In this design of the experiment, we intentionally pre-schedule the above two

events only for the purpose of demonstrating the essence of the research. The browser being applied in the following experiments was the *Safari* with version 5.1.7 (7534.57.2).

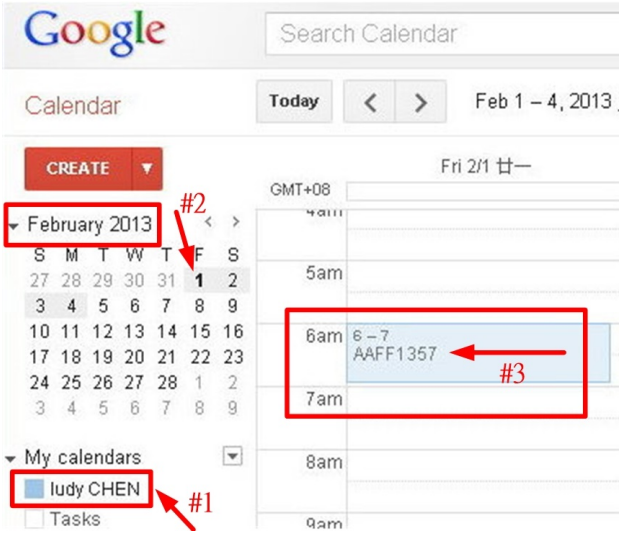

Figure 1. The screen shot of the event scheduled on 1 February 2013.

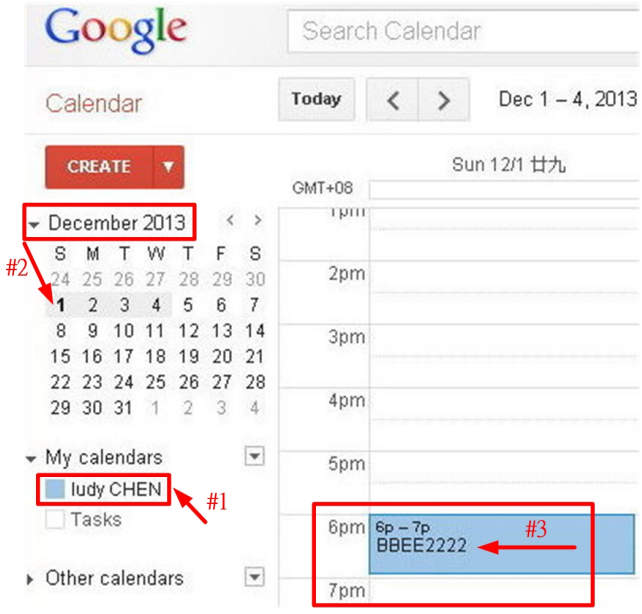

Figure 2. The screen shot of the event scheduled on 1 December 2013.

Phase 2: The DF team rebooted the computing device and manually eliminated all cache data within the *Safari* browser before each operation in order to consolidate that there is no historical digital trails being accidentally accumulated. The computing device of the experiment for each case in the following section was conducted on the notebook. At last, the DF team purged any e-mails left in the Gmail e-mail boxes to avoid the possible residuals of the associate digital trails, which could affect the outcome(s) of the experiment.

For the simplicity of representing the essence of the research, the DF team formalized the following expressions with respect to the major two factors of the experiments, which are the execution status of the *Google Calendar* and *Safari*. Hence, we intentionally present the following representations:

Let £ be the integration function concerning the objects, *CRE*, *C*, *S*, and *T*.

- The attributes of CRE_i represent the corresponding C_j, S_k, and $T^m{}_n$ objects were not newly created for $i = 0$ and the associate *C* object was recently generated for $i = 1$.
- The attributes of C_j represent *Google Calendar* is active during the digital evidence collection for $j = 1$ and *Google Calendar* is logout for $j = 0$, respectively.
- The attributes of S_k represent *Safari* is active during the digital evidence collection for $k = 1$ and *Safari* is logout for $k = 0$, correspondingly.
- The attributes of $T^m{}_n$ represents the target string that has been visualized during the digital evidence collection for $m = 1$ and the target string has not been visualized for $m = 0$, respectively. When $m = -1$, it represents there is no visualization of the marked itinerary. Lastly, n is string being targeting.

Case 1: Google Calendar and Safari are still activated with the visualization of the event marked on 1 February 2013 only

Step 1: The DF team initially logged on to *Google Calendar* using the account, *ludy099122@gmail.com*. We can be informed that the user name of the current user is *ludy CHEN* as the arrow #1 points in Figure 1. Furthermore, we firmly visualize the event marked on 1 February 2013 as arrow #2 points in Figure 1. As arrow #3 points in Figure 1, the posted event is *AAFF1357* between 6:00 a.m. and 7:00 a.m.

Step 2: The DF team utilized the *Helix® Ver. 2.0* (e-fense, Washington, DC, USA) to acquire the image file of the RAM of the computing device. The image file, *case_1.dd*, was obtained with file size 536,211,456 Bytes (523,644 KB).

Step 3: The DF team utilized the forensics sound toolkit, *ProDiscover Basic® Version 4.8a* (ARC Group, New York, NY, USA) to parse the image file of the RAM, *case_1.dd*, and applied the specific search keyword to search the image file of the RAM.

By the virtue of sophisticated accumulated experience, the DF team applied the search keyword, *passwd=*, with respect to the image file of the computing device in order to conduct the data carving procedure to disclose the related digital trails. The search results turn 10 hits in 10 files as Figure 3 indicated and the password for the current *Gmail* user was disclosed to be *09182012* as arrow #1 points. We can also additionally identify that the current *Gmail* user was *ludy099122* as arrow #2 indicates.

In addition, we explored the possible outcome(s) with respect to the planned itinerary using the search keyword, *AAFF1357*, concerning to the image file of the RAM of the computing device. The search results turn negative. This demonstrates that even the pre-scheduled itinerary had been visualized via the browser, there is no digital trail regarding that event. Furthermore, we apply another search keyword, *BBEE2222*, the search result also turn negative, which demonstrates that even without the visualization of the pre-scheduled itinerary via the browser, there is still no digital trail concerning that event. Consequently, we have the following representations for the outcome of this case:

$$£(CRE_0, C_1, S_1, T^{-1}{}_{passwd=}) = 10$$
$$£(CRE_0, C_1, S_1, T^{1}{}_{AAFF1357}) = 0$$
$$£(CRE_0, C_1, S_1, T^{0}{}_{BBEE2222}) = 0$$

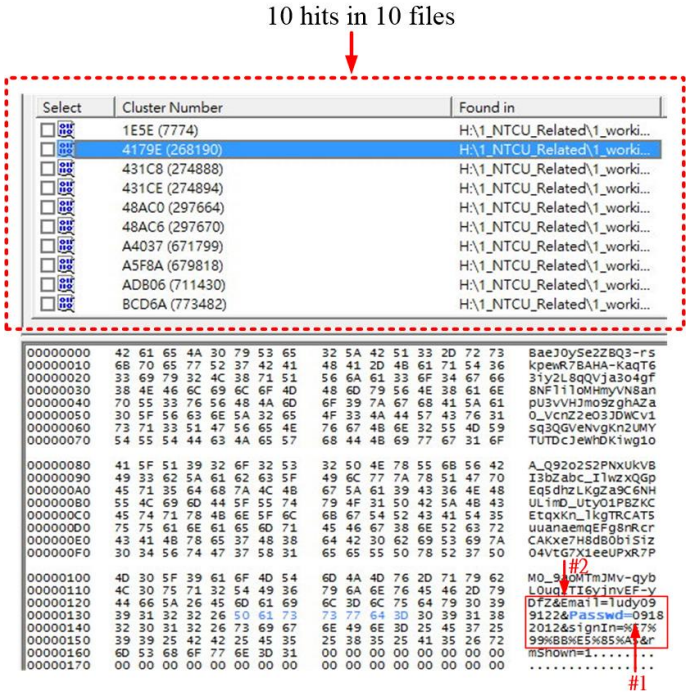

Figure 3. The results of data carving reveal the id and password for the previous *Gmail* session.

Case 2: Rebooting the notebook with both Google Calendar and Safari is still activated without the visualization via the browser of the event marked on 1 February 2013

Step 1–Step 3: Experiments were conducted identically as those procedures in *Case 1*.

The DF team conducted the digital evidence collection under the premise that the users did not log out of *Gmail* and leaving *Safari* browser still running without the visualization of the previous event in contrast to the previous case.

The DF team applies search keyword, *passwd*=, the search results turn 12 hits in 12 files as Figure 4 shows. The Gmail user ID and password are also capable of being disclosed as in *Case 1*.

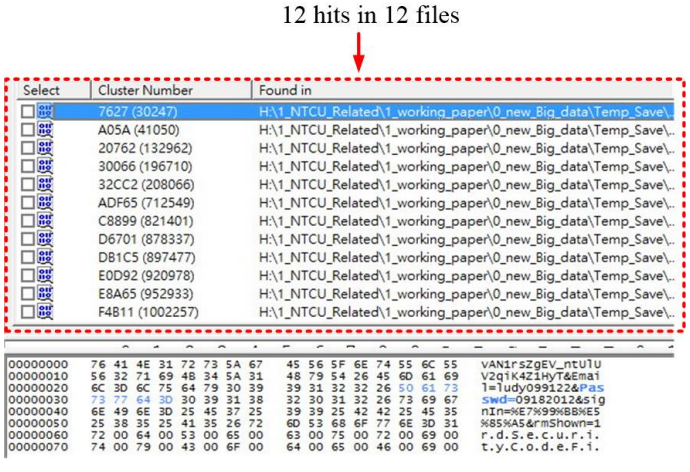

Figure 4. The results of data carving turn 12 hits in 12 files concerning the search keyword, *passwd*=.

If we applied *AAFF1357*, the search results turn negative.

If we applied *BBEE2222*, the search results also turn negative.

Hence, we have the following representation for the outcomes of this case.

$$\pounds(CRE_0, C_1, S_1, T^{-1}{}_{passwd=}) = 12$$
$$\pounds(CRE_0, C_1, S_1, T^{1}{}_{AAFF1357}) = 0$$
$$\pounds(CRE_0, C_1, S_1, T^{0}{}_{BBEE2222}) = 0$$

Case 3: Rebooting the notebook with Google Calendar being logout and Safari shutdown after the visualization of the event marked on 1 February 2013

Step 1–Step 3: Experiments were conducted identically as those procedures in *Case 1*.

Applying the search keyword, *passwd=*, the search results turn 4 hits in 4 files as Figure 5 illustrates. Furthermore, following the same procedure as the aforementioned one in the previous case, the user ID and passwords of the current *Gmail* session is not capable of being discovered.

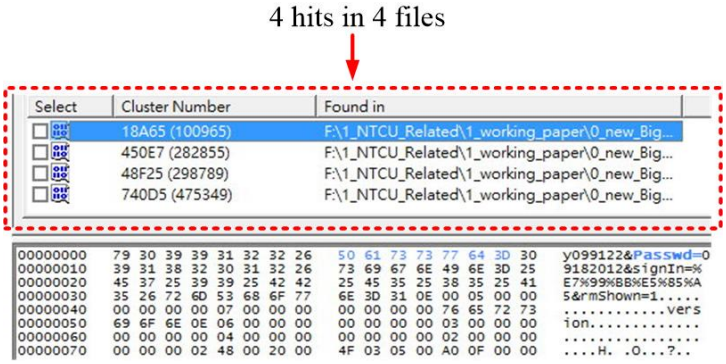

Figure 5. The results of data carving turn 4 hits in 4 files concerning the search keyword, *passwd=*.

If we applied *AAFF1357*, the search results turn negative.

If we applied *BBEE2222*, the search result also turn negative. Accordingly, we have the following representation for this case.

$$\pounds(CRE_0, C_0, S_0, T^{-1}{}_{passwd=}) = 4$$
$$\pounds(CRE_0, C_0, S_0, T^{1}{}_{AAFF1357}) = 0$$
$$\pounds(CRE_0, C_0, S_0, T^{0}{}_{BBEE2222}) = 0$$

Case 4: Rebooting the notebook with both Google Calendar and Safari is still activated with the newly created event on 1 May 2013 with the event string KKYY8899 between 6:00 a.m. and 7:00 a.m.

Step 1–Step 3: Experiments were conducted identically as those procedures in *Case 1*.

We applied the *KKYY8899* as the search keyword, the research result turn 24 hits in 24 files as Figure 6 demonstrates.

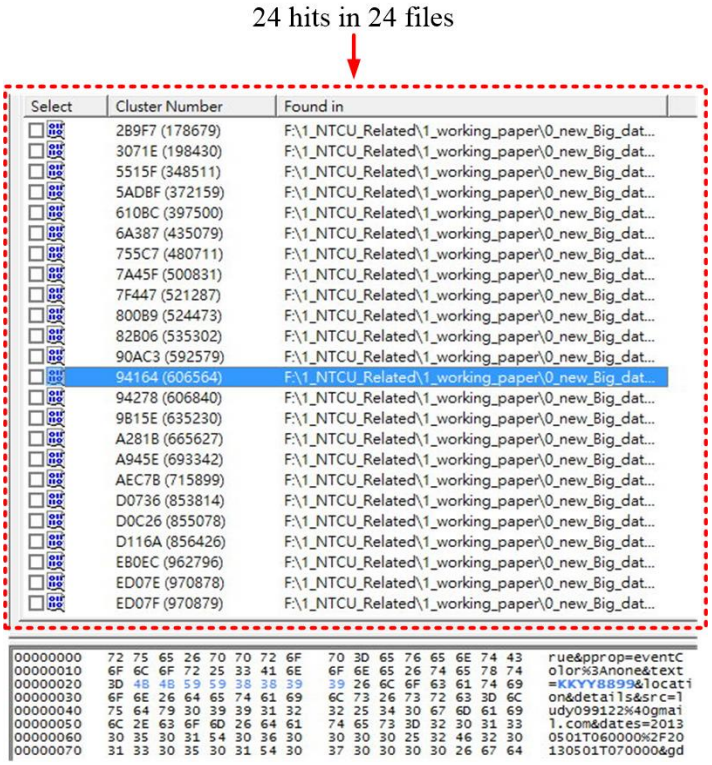

Figure 6. The results of data carving turn 24 hits in 24 files concerning the search keyword, *KKYY8899*.

If we applied the search keyword, *passwd*=, the search result turn 10 hits in 10 files as Figure 7 demonstrates.

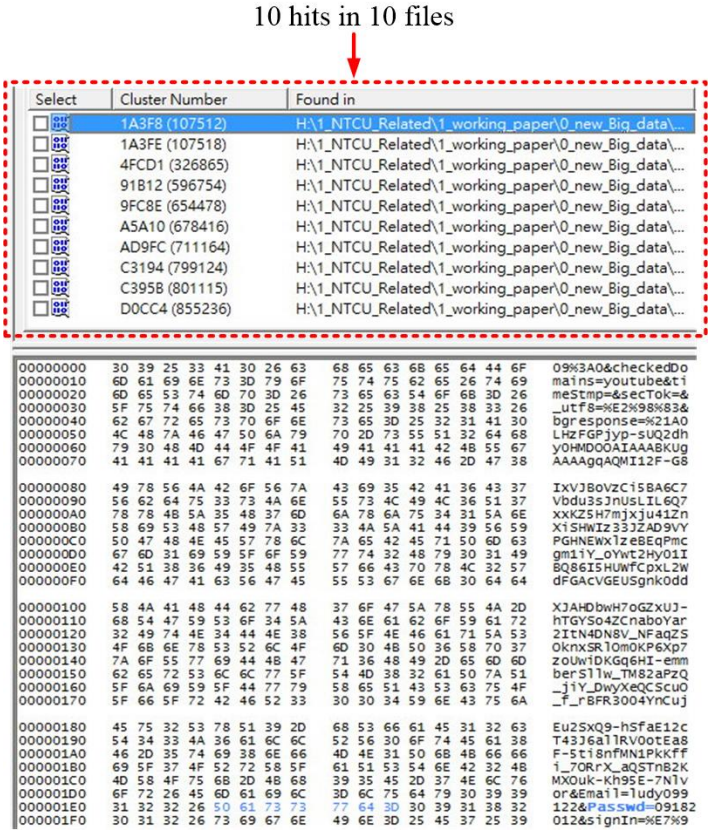

Figure 7. The results of data carving turn 10 hits in 10 files concerning the search keyword, *passwd*=.

If we applied *AAFF1357*, the search results turn negative.

If we applied *BBEE2222*, the search results also turn negative.

Therefore, we illustrate the experiments in the following concise formats.

$$£(CRE_1, C_1, S_1, T^{-1}{}_{passwd=}) = 10$$
$$£(CRE_1, C_1, S_1, T^{1}{}_{KKYY8899}) = 24$$
$$£(CRE_1, C_1, S_1, T^{0}{}_{AAFF1357}) = 0$$
$$£(CRE_1, C_1, S_1, T^{0}{}_{BBEE2222}) = 0$$

Case 5: Rebooting the notebook and then conduct acquiring the image file of the RAM with both Google Calendar and Safari are active without the visualization of pre-arranged events on 1 February 2013 or 1 December 2013.

Step 1–Step 3: Experiments were conducted identically as those procedures in *Case 1*.

If we applied the search keyword, *passwd=*, the search results turn negative.

If we applied the search keyword, *AAFF1357*, the search results turn negative.

If we applied the search keyword, *BBEE2222*, the search result turns negative.

If we applied the search keyword, *KKYY8899*, the search result turns negative.

The above digital evidences suggest that the volatile digital evidences are vanished once the power of the computing devices is no longer sustainable.

Consequently, we have the following symbolic representations for this case.

$$£(CRE_0, C_1, S_1, T^{-1}{}_{passwd=}) = 0$$
$$£(CRE_0, C_1, S_1, T^{1}{}_{KKYY8899}) = 0$$
$$£(CRE_0, C_1, S_1, T^{0}{}_{AAFF1357}) = 0$$
$$£(CRE_0, C_1, S_1, T^{0}{}_{BBEE2222}) = 0$$

4. Summaries among Cases

Figure 8 summarizes the above-mentioned five cases in a succinct manner with synthesis and analysis of the aforementioned five cases via the tree structure. The Figure suggests the following statements:

***Case 1*:** When the DF specialists collect the associate digital evidences, if both *Google Calendar* and *Safari* are both activated with the visualization of the event marked on 1 February 2013, the pre-arranged itinerary, the DF team is not capable of disclosing the digital traces on both pre-arranged events. But, the passwords for the current *Google* session (10 hits in 10 files) will be able to be revealed.

***Case 2*:** When the DF specialists collect the associate digital evidences, if both *Google Calendar* and *Safari* are both activated without the visualization on 1 February 2013, the DF team is also able to disclose the passwords (12 hits in 12 files) of the current *Gmail* session.

***Case 3*:** If both *Google Calendar* and *Safari* are both shutdown even with the visualization of the event marked on 1 February 2013, the pre-arranged itinerary, the DF team is not capable of disclosing the digital traces on both pre-arranged events. In addition, the DF team is still able to reveal the passwords (4 hits in 4 files) of the current *Gmail* session.

***Case 4*:** If both *Google Calendar* and *Safari* are both activated with the newly created event on the spot when the DF team collects the digital trails, the DF team is still not able to disclose the pre-arranged

events. Additionally, the DF team is capable of discovering the digital traces concerning the newly generated one with 24 hits in 24 files. Furthermore, the DF team is also able to disclose the passwords (24 hits in 24 files) of the current *Gmail* session.

***Case 5*:** If the computing device has been rebooted, the volatile memory will be vanished forever. Alternatively, there will be no digital trails disclosed at this stage.

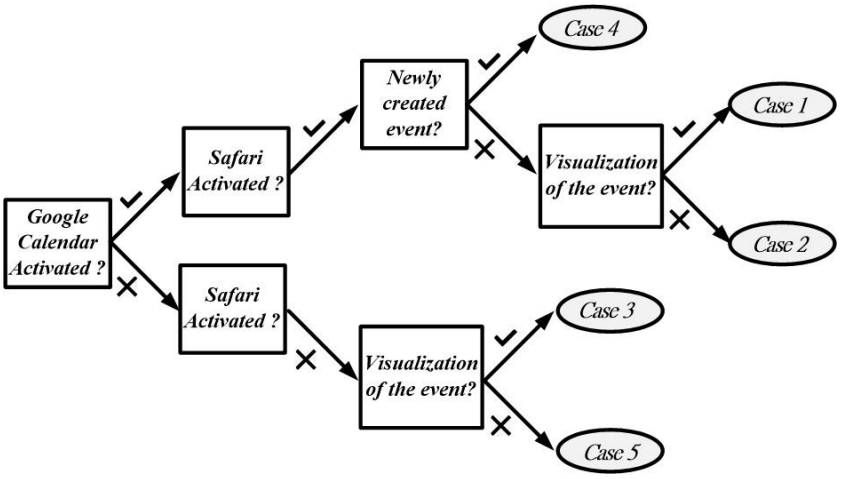

Figure 8. The summaries of the aforementioned five cases via the tree structure.

5. Conclusions

As *Google Calendar* and *Safari* are extensively utilized by voluminous web participants, digital trails are unwarily and accidently left within the computing devices and they could be systematically and scientifically, disclosed, and analyzed via the associate digital forensics procedures as we exhibited in this research paper, which was demonstrated by the combination of different scenarios with *Google Calendar* and the *Safari* browser. Illustrated by this paper, we can conclude that as long as the DF specials obtain the image of the RAM of the computing device, there will be a high possibility to present sufficient evidences to testify the suspects in terms of some cybercrimes in a court of law. In addition, we can tell that the password of the current *Gmail* session could be disclosed as long as the computing device has not been shut down or rebooted. On the other hand, whether the suspect visualizes the specific event of *Google Calendar* or not, there is no way to disclose the pre-arranged itineraries. However, if the event was just created on the spot, it is feasible to disclose the digital traces to prove that the suspect actually committed this behavior on the spot as probative evidences.

Acknowledgment

The authors would like to acknowledge the funding support of Ministry of Science and Technology (MOST), Taiwan.

Author Contributions

Hai-Cheng Chu wrote the draft of the paper; Gai-Ge Wang suggested the research directions; and Jong Hyuk Park contributed to the initial design of the experiment and the revision for this research publication.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Casey, E. Common pitfalls of forensic processing of blackberry mobile devices, 2009. Available online: http://computer-forensics.sans.org/blog/2009/06/15/common-pitfalls-of-forensic-processing-of-blackberry-mobile-devices# (accessed on 22 December 2014).
2. Al-Saleh, M.I.; Al-Sharif, Z.A. Utilizing data lifetime of TCP buffers in digital forensics: Empirical study. *Digit. Investig*. **2012**, *9*, 119–124.
3. Olajide, F.; Savage, N.; Shoniregun, C. Digital Forensic Research—The Analysis of User Input on Volatile Memory of Windows Application. In Proceedings of 2012 World Congress on Internet Security, Guelph, Canada, 10–12 June 2012; pp. 231–238.
4. Becker, A.; Mladenow, A.; Kryvinska, N.; Strauss, C. Aggregated survey of sustainable business models for agile mobile service delivery platforms. *J. Serv. Sci. Res.* **2012**, *4*, 97–121.
5. Halderman, J.; Schoen, S.; Heninger, N.; Clarkson, W.; Paul, W.; Calandrino, J.; Feldman, A.; Appelbaum, J.; Felten, E. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM Secur. Browser* **2009**, *52*, 91–98.
6. He, M.; Fang, J.; Jiang, Z.L.; Yiu, S.M.; Chow, K.P.; Niu, X. Digital forensic on MTK-based shanzhai mobile phone with nand flash. In Proceedings of the First International Conference on Digital Forensics and Investigation, Beijing, China, 21–23 September 2012; pp. 1–10.
7. Damopoulos, D.; Kambourakis, G.; Gritzalis, S. From keyloggers to touchloggers: Take the rough with the smooth. *Comput. Secur.* **2013**, *32*, 102–114.
8. Tso, Y.C.; Wang, S.J.; Huang, C.T.; Wang, W.J. iPhone social networking for evidence investigations using iTunes forensics. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. ICUIMC'12, Kuala Lumpur, Malaysia, 20–22 February 2012; pp. 1–7.
9. Owen, P.; Thomas, P. An analysis of digital forensic examinations: Mobile devices *versus* hard disk drives utilizing ACPO & NIST guidelines. *Digit. Investig*. **2011**, *8*, 135–140.
10. Casey, E.; Bann, M.; Doyle, J. Introduction to windows mobile forensics. *Digit. Investig*. **2010**, *6*, 136–146.
11. Kim, D.; Park, J.; Lee, K.; Lee, S. Forensic analysis of android phone using ext4 file system journal log. *Future Inf. Technol. Appl. Service LNEE* **2012**, *164*, 435–446.
12. Grispos, G.; Storer, T.; Glisson, W.B. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digit. Investig*. **2011**, *8*, 23–26.
13. Conti, G.; Bratus, S.; Shubina, A.; Sangster, B.; Ragsdale, R.; Supan, M.; Lichtenberg, A.; Perez-Alemany, R. Automated mapping of large binary objects using primitive fragment type classification. *Digit. Investig*. **2010**, *7*, S3–S12.
14. Chun, W.; Park, D. A study on the forensic data extraction method for SMS, photo and mobile image of Google android and windows mobile smart phone. *Converg. Hybrid Inf. Technol. CCIS* **2012**, *310*, 654–663.

15. Casey, E. *Digital Evidence and Computer Crime*; Academic Press: New York, NY, USA, 2011.
16. Arrifin, A.; D'Orazio, C.; Choo, K.R.; Slay, J. IOS forensics: How can we recover deleted image files with timestamp in a forensically sound manner? In Proceedings of 2013 8th International Conference on Availability, Reliability and Security, Regensburg, Germany, 2–6 September 2013; pp. 375–382.
17. Lohrum, M. Forensic extractions of data from the Nokia N900. *Digit. Forensics Cybercrime LNICST* **2012**, *88*, 89–103.
18. Höbarth, S.; Mayrhofer, R. A framework for on-device privilege escalation exploit execution on android. In Proceedings of IWSSI/SPMU 2011: 3rd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, San Francisco, CA, USA, 12 June 2011.
19. Ayers, R.; Brothers, S.; Jansen, W. *Guidelines on Mobile Device Forensics*; National Institute of Standards and Technology (NIST) SP 800; U.S. Department of Commerce: Washington, DC, USA, 2014; pp. 1–67.
20. Lessard, J.; Kessler, G.C. Android forensics: Simplifying cellphone examinations. *Small Scale Digit. Device Forensic J.* **2010**, *4*, 1–12.
21. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73.