

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).

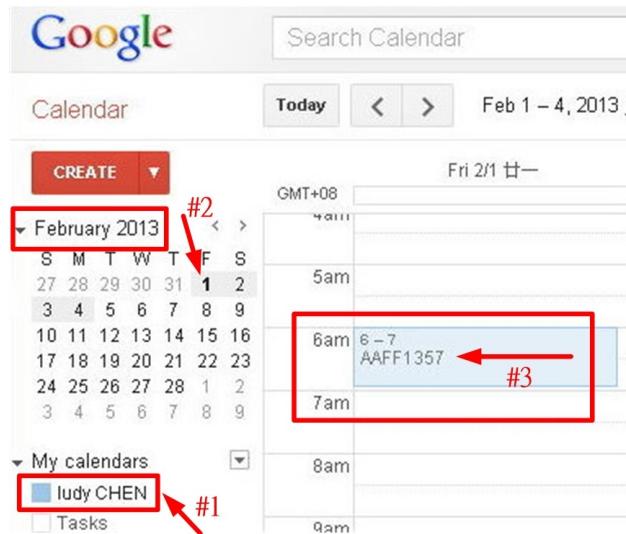


Figure 1. The screen shot of the event scheduled on 1 February 2013.

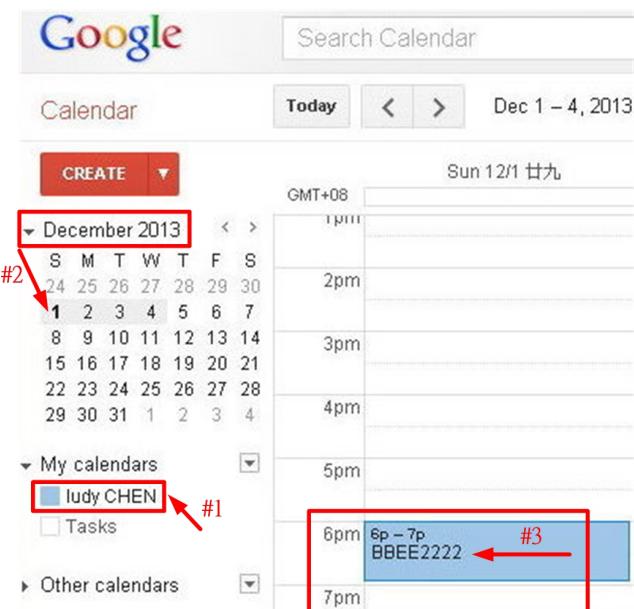


Figure 2. The screen shot of the event scheduled on 1 December 2013.

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 \mathcal{L} 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:

$$\mathcal{L}(CRE_0, C_1, S_1, T^{-1}_{passwd=}) = 10$$

$$\mathcal{L}(CRE_0, C_1, S_1, T^1_{AAFF1357}) = 0$$

$$\mathcal{L}(CRE_0, C_1, S_1, T^0_{BBEE2222}) = 0$$

10 hits in 10 files										
Select	Cluster Number	Found in								
<input type="checkbox"/>	1E5E (7774)	H:\1\NTCU_Related\1\worki...								
<input checked="" type="checkbox"/>	4179E (268190)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	431C8 (274888)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	431CE (274894)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	48AC0 (297664)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	48AC6 (297670)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	A4037 (671799)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	A5F8A (679818)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	ADB06 (711430)	H:\1\NTCU_Related\1\worki...								
<input type="checkbox"/>	BCD6A (773482)	H:\1\NTCU_Related\1\worki...								
00000000	42 62 65 44 30 79 53 65	32 5A 42 51 33 2D 72 73	BaeJ0ySeZzBQ3-rs							
00000010	68 70 65 77 52 37 42 41	48 41 2D 46 61 71 54 66	kpewR7BAh-KaqT6							
00000020	33 69 79 32 4C 38 71 51	56 6A 61 33 6F 34 67	31yL2qVjQz3a4gF							
00000030	38 4E 46 62 69 6C 6F 40	49 6D 79 5A 50 42 48 38	VNF11oWm9zVNVn8an							
00000040	70 55 33 76 56 48 4A 60	6F 39 7A 68 64 41 5A 61	pu3VVHjm9zghAza							
00000050	30 5F 56 63 6E 5A 32 65	4F 33 49 44 57 43 76	0_vCvD2e03d3f							
00000060	73 54 53 42 56 65 46	70 49 48 52 36 55 40	59 70 69 63 62 61							
00000070	54 55 53 44 48 44 65 37	74 44 48 69 67 67 51	TUDTCJewDfK1wNg1o							
00000080	41 5F 51 39 32 6F 32 53	32 50 4E 78 55 6B 56 42	A_Q92z02P5NzKuVb							
00000090	49 33 62 5A 61 62 63 5F	49 6C 77 7A 78 51 47 70	I3bzabc_7WqzXGp							
000000A0	45 71 35 64 68 7A 4C 4B	67 5A 61 39 43 36 4E	E5d5LzLqzCa3c6N							
000000B0	55 4C 69 60 44 55 75 74	79 4F 31 50 42 52 48 43	ULIn-0tY_01PBzKC							
000000C0	45 74 71 78 4B 6E 5F 6C	68 67 54 52 43 41 54 35	EtqxKnn_1kgTrCATS							
000000D0	75 75 61 66 65 65 70 71	46 46 67 32 66 52 63 72	uaanameqFg8nR1rcz							
000000E0	43 41 48 78 65 37 48 38	64 42 30 62 59 63 69 7A	CAKxe7H8BD0B1rCz							
000000F0	30 54 56 74 47 37 58 31	65 65 55 50 78 52 57 39	04VqfzJ0eUPXr#							
00000100	40 30 5F 39 61 6F 4D 54	60 4A 4D 76 2D 71 79 62	MO_3qMjTMjMq-yqb							
00000110	4C 30 75 71 32 54 49 36	79 6A 6E 76 45 46 29 70	LouqTi6yJn1nFEV-							
00000120	44 66 5A 26 45 6D 61 69	6C 3D 6C 75 64 79 30 39	D724@mail.ru:109y							
00000130	39 31 32 32 26 50 61 73	73 77 64 3D 30 39 31 38	9122+&Passwd=0918							
00000140	32 30 31 32 26 73 69 67	6E 49 6E 30 25 45 37 25	2012+&SignIn=99%							
00000150	39 39 25 42 42 25 45 35	28 35 38 25 41 35 26 72	99%&BME5%85\$5&r							
00000160	60 53 68 67 77 66 3D 31	00 00 00 00 00 00 00 00	mShowN=1.....							
00000170	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	#1							

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*.

Select	Cluster Number	Found in
<input type="checkbox"/>	7627 (30247)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	A05A (41050)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	20762 (132962)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	30066 (196710)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	32C2C (208066)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	ADF65 (712549)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	C8899 (821401)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	D6701 (878337)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	DB1C5 (897477)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	ED9D2 (920978)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	E8A65 (952933)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\
<input type="checkbox"/>	F4B11 (1002257)	H:\1_NTCU_Related\1_working_paper\0_new_Big_data\Temp_Save\

00000000	76	41	4E	31	72	73	5A	67	45	56	5F	6E	74	55	6C	55	VAN1#zSgEV_ntulu
00000010	56	32	71	69	48	34	51	31	48	54	26	45	60	61	69	V2q1K4Z1H7E@mail	
00000020	6C	3D	65	64	79	30	39	39	31	32	32	26	50	61	73	I=udy091122&pas	
00000030	73	76	64	30	39	31	38	32	30	31	32	26	73	69	67	sd=09182012&61g	
00000040	25	38	35	35	41	35	45	26	72	60	53	68	77	66	30	31	
00000050	25	38	35	35	41	35	45	26	72	60	53	68	77	66	30	%\$5%AS&#nshowone1	
00000060	72	00	64	00	53	00	66	00	63	00	75	00	72	00	69	00	
00000070	74	00	79	00	43	00	66	00	64	00	65	00	66	00	69	t.y.c.o.d.e.f.i.	

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.

$$\begin{aligned} \ell(CRE_0, C_1, S_1, T^{-1}_{passwd}) &= 12 \\ \ell(CRE_0, C_1, S_1, T^1_{AAFF1357}) &= 0 \\ \ell(CRE_0, C_1, S_1, T^0_{BBEE2222}) &= 0 \end{aligned}$$

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.

4 hits in 4 files



Select	Cluster Number	Found in
<input checked="" type="checkbox"/>	18A65 (100965)	F:\1_NTCU_Related\1_working_paper\0_new_Big...
<input type="checkbox"/>	450E7 (282855)	F:\1_NTCU_Related\1_working_paper\0_new_Big...
<input type="checkbox"/>	48F25 (298789)	F:\1_NTCU_Related\1_working_paper\0_new_Big...
<input type="checkbox"/>	740D5 (475349)	F:\1_NTCU_Related\1_working_paper\0_new_Big...

00000000	79	30	39	39	31	32	32	26	50	61	69	73	73	6E	49	64	3D	30	91y099122&SignIn=0
00000010	39	31	38	32	30	31	32	26	73	69	73	73	6E	49	64	3D	30	91y099122&SignIn=0	
00000020	45	37	25	39	39	25	42	42	25	45	35	25	38	35	25	41	E7%99%BB%E5%85%KA		
00000030	35	26	72	60	53	68	6F	77	6E	3D	31	00	05	00	00	00	54&rmsShown=1		
00000040	00	00	00	00	07	00	00	00	00	00	00	00	76	65	72	73vers	
00000050	69	6F	6E	0E	06	00	00	00	00	00	00	00	03	00	00	00	ion.....	
00000060	00	00	00	00	04	00	00	00	00	00	00	00	02	00	00	00H..O...?..	
00000070	00	00	00	02	48	00	20	00	4F	03	05	00	A0	0F	00	00	

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.

$$\begin{aligned} f(CRE_0, C_0, S_0, T^{-1}_{passwd}) &= 4 \\ f(CRE_0, C_0, S_0, T^1_{AAFF1357}) &= 0 \\ f(CRE_0, C_0, S_0, T^0_{BBEE2222}) &= 0 \end{aligned}$$

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.

24 hits in 24 files		
Select	Cluster Number	Found in
<input type="checkbox"/>	2B9F7 (178679)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	3071E (198430)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	5515F (348511)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	5ADBF (372159)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	610BC (397500)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	6A387 (435079)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	755C7 (480711)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	7A45F (500831)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	7F447 (521287)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	80089 (524473)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	82B06 (535302)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	90AC3 (592579)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input checked="" type="checkbox"/>	94164 (606564)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	94278 (606840)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	9815E (635230)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	A281B (665627)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	A945E (693342)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	AEC7B (715899)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	D0736 (855814)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	D0C26 (855078)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	D116A (856426)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	E80EC (962796)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	ED07E (970878)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...
<input type="checkbox"/>	ED07F (970879)	F:\1_NTCU_Related\1_working_paper\0_new_Big.dat...

00000000	72 75 65 26 70 70 72 6F	70 3D 65 76 65 6E 74 43	rue&prop=eventC
00000010	6F 6C 6F 72 25 33 41 6E	6F 6E 65 26 74 65 78 74	olor%3Anone&text
00000020	3D 4B 4B 59 59 38 38 39	39 26 6C 6F 63 61 74 69	=KKYY8899&locat
00000030	6F 6E 26 64 65 74 61 69	6C 73 26 73 72 63 3D 6C	on&details&src=1
00000040	75 64 79 30 39 31 32	32 25 34 30 67 6D 61 69	udy099122%40gmai
00000050	6C 2E 63 6F 6D 26 64 61	74 65 73 3D 32 30 31 33	1.comdates=2013
00000060	30 35 30 31 54 30 36 30	30 30 30 25 32 46 32 30	0501T060000%2F20
00000070	31 33 30 35 30 31 54 30	37 30 30 30 30 26 67 64	130501T070000%gd

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.

10 hits in 10 files		
Select	Cluster Number	Found in
<input type="checkbox"/>	1A3F8 (107518)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	1A3FE (107518)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	4FCDF1 (326865)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	91B12 (596754)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	9FC8E (654478)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	ASA10 (678416)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	AD9FC (711164)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	C3194 (799124)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	C395B (801115)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...
<input type="checkbox"/>	D0CC4 (855236)	H:\1_NTCU_Related\1_working_paper\0_new_Big.data...

00000000	30 39 25 33 41 30 26 63	68 65 63 68 65 64 44 6F	09%3A&checked=0
00000010	6D 61 69 73 3D 79 6F	77 64 75 62 65 26 14 29	main= youtube&t1
00000020	6D 65 53 74 6D 70 3D 6E	73 65 63 54 6F 28 3D 30	meStamp=&secTok=&
00000030	25 48 44 66 38 3D 25 45	25 29 39 28 25 38 33 26	_utf8=%E2%98%83&
00000040	62 67 72 65 73 70 6F 6E	73 65 3D 25 32 31 41 30	bqr=response=<21AO
00000050	4C 48 7A 46 47 50 6A 79	70 20 73 55 51 32 64 68	LHZFGPjyp-sUQ2dh
00000060	79 30 48 4D 44 4F 4F 41	49 41 41 41 42 48 55 67	yOHMD0AIAAABKUG
00000070	41 41 41 41 67 71 41 51	40 49 31 32 46 2D 47 38	AAAAGqAQMI12F-G8
00000080	49 78 56 4A 56 7A	43 69 35 42 41 36 43 37	IxVJBovZC15BA6C7
00000090	56 62 64 75 33 73 4A 6E	55 73 4C 49 4C 36 51 37	VbdU3sJnUSLIL607
000000A0	78 78 4B 5A 55 48 37 6D	6A 76 6A 75 34 31 5A 6E	XXKZS7HmjxU412n
000000B0	58 69 53 48 57 49 7A 33	33 44 5A 41 44 39 56 59	X1SHWIZ33J2AD9VV
000000C0	50 47 48 4E 45 57 78 6C	7A 65 42 45 71 50 6D 63	PGHNEWX1eBEqPmc
000000D0	67 6D 31 69 59 5F 68 59	77 74 32 48 79 30 31 49	gm1Y_OYwt2Hy01I
000000E0	42 51 38 36 49 35 48 55	57 66 43 70 78 4C 32 57	BQ8615HUWTpxL2W
000000F0	64 46 47 41 63 56 47 45	55 53 67 6E 6B 30 64 64	dFGAcVGEGUSEgnkodd
00000100	58 4A 41 48 44 62 77 48	37 6F 47 5A 78 55 4A 2D	XAHDbwH7oGZxUJ-
00000110	68 54 47 59 53 6F 34 5A	43 66 61 62 6F 59 64 72	VBdU3sJnUSLIL607
00000120	32 49 44 4E 45 44 4E 38	56 5F 4E 46 61 51 5A 53	2ITN4DNBV_NFa025
00000130	4F 48 6E 78 53 52 6C 5F	60 50 48 50 26 58 30 37	OknxSR1omOKP6Xp07
00000140	7A 6F 55 77 69 44 4B 47	71 36 48 49 2D 65 60 60	zOUwiDKGq6HI-emm
00000150	62 65 53 6C 77 5F	54 50 38 32 61 50 7A 51	berS1Lw_TM82aPzQ
00000160	5F 6A 69 59 5F 44 77 79	58 65 51 43 53 63 75 4F	j1Y_DwyXeQCScu0
00000170	5F 66 5F 72 42 46 52 33	30 30 34 59 6E 43 75 6A	___.BFR3004YnCuJ
00000180	45 75 32 53 78 51 39 2D	68 53 66 61 45 31 32 63	Eu2SxQ9-hsfiae12c
00000190	54 34 33 4A 36 61 6E 6C	52 56 30 6F 74 45 61 38	T43J6allRVootEa8
000001A0	46 20 35 74 69 38 6E 66	40 4E 31 50 6B 4B 66 66	F-5t18nfMNN1PKff
000001B0	69 5F 37 4F 52 72 58 5F	61 53 53 54 6E 42 32 48	i_7ORx_aqSTnB2k
000001C0	40 58 4F 75 6B 2D 48 68	39 35 45 2D 37 4E 6C 76	MXOUk-Kh95E-7N1v
000001D0	6F 72 26 45 6D 61 69 6C	30 6C 75 64 79 30 39 39	or &Email=udy099
000001E0	31 32 32 26 50 61 73 73	77 64 3D 30 39 31 38 32	122&passwd=09182
000001F0	30 31 32 26 73 69 67 6E	49 6E 3D 25 45 37 25 39	012&signIn=%E7%9

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.

$$\begin{aligned}\mathcal{L}(CRE_1, C_1, S_1, T^{-1}_{passwd=}) &= 10 \\ \mathcal{L}(CRE_1, C_1, S_1, T^1_{KKYY8899}) &= 24 \\ \mathcal{L}(CRE_1, C_1, S_1, T^0_{AAFF1357}) &= 0 \\ \mathcal{L}(CRE_1, C_1, S_1, T^0_{BBEE2222}) &= 0\end{aligned}$$

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.

$$\begin{aligned}\mathcal{L}(CRE_0, C_1, S_1, T^{-1}_{passwd=}) &= 0 \\ \mathcal{L}(CRE_0, C_1, S_1, T^1_{KKYY8899}) &= 0 \\ \mathcal{L}(CRE_0, C_1, S_1, T^0_{AAFF1357}) &= 0 \\ \mathcal{L}(CRE_0, C_1, S_1, T^0_{BBEE2222}) &= 0\end{aligned}$$

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.

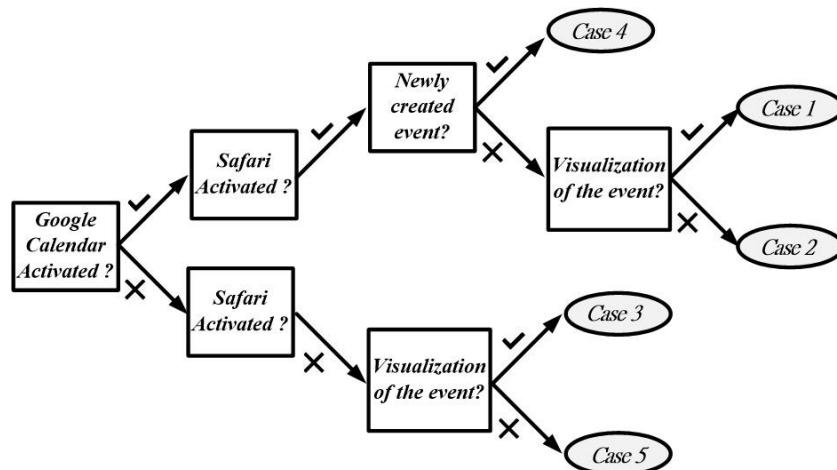


Figure 8. The summaries of the aforementioned five cases via the tree structure.

5. Conclusions

As *Google Calendar* and *Safari* are extensively utilized by voluminous web participants, digital trails are unwarily and accidentally 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. Grisplos, 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 LNCS* **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.

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).