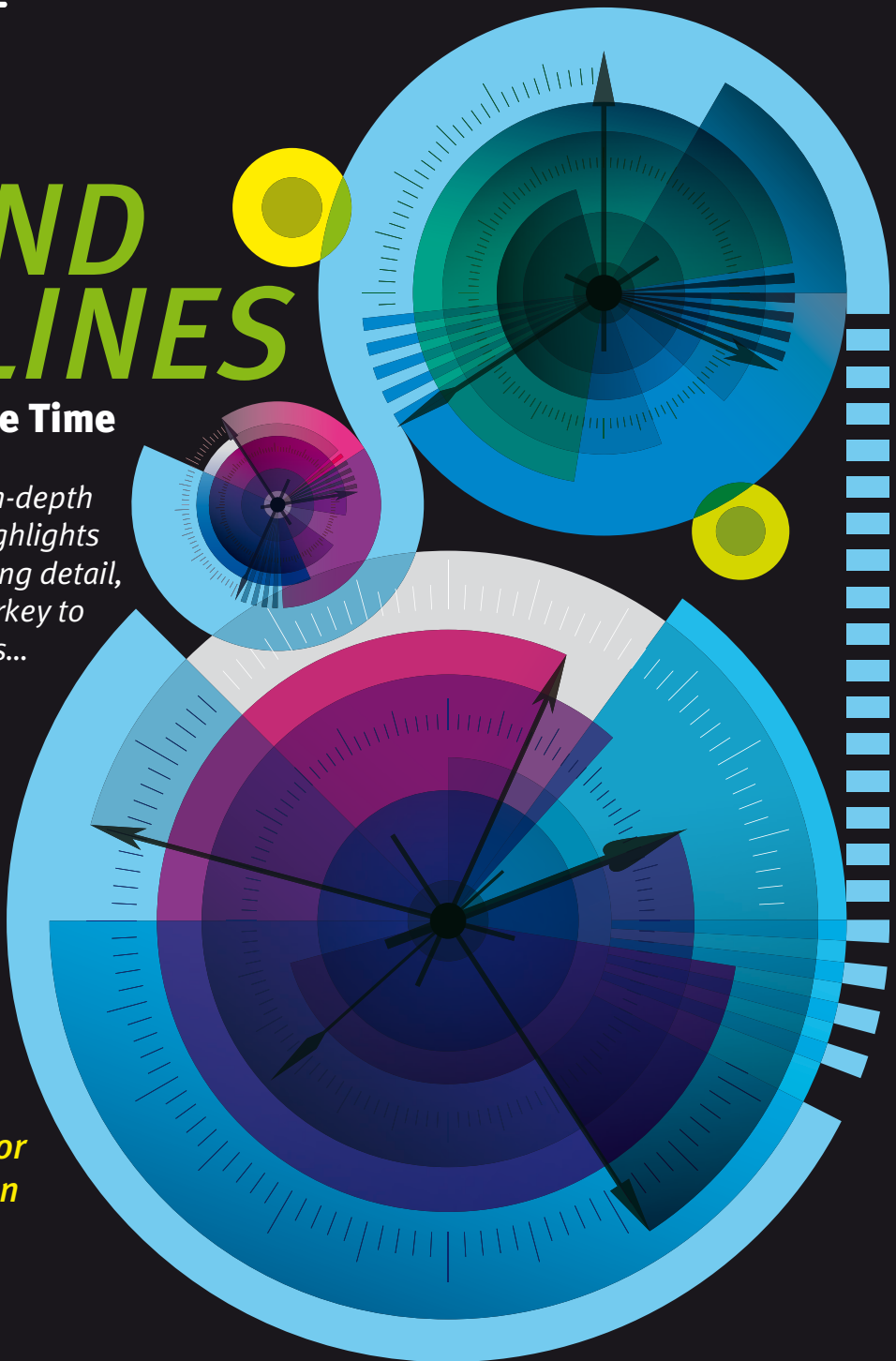
The Quarterly Magazine for Digital Forensics Practitioners

Issue 18 • February 2014

DIGITAL FORENSICS / MAGAZINE

WIN! an iPod Nano



BEYOND TIMELINES

Anchors in Relative Time

Mark Spencer takes an in-depth look at timelines, and highlights the importance of checking detail, using a recent case in Turkey to demonstrate the dangers...

Latest News, 360
Book Reviews, IRQ
& much more inside!

PLUS!

Forensic Readiness
Malicious use of Android Permissions
Using Fuzzy Hashes for Malware Classification

9 772042 061004 18
Issue 18 / £14.99 TR Media

BEYOND TIMELINES
ANCHORS IN RELATIVE TIME

What happens to our timelines when we have reason to believe that critical dates and times within our evidence cannot be trusted, not even to be consistently inaccurate? Mark Spencer explains...

/ INTERMEDIATE

Digital forensics and incident response (DFIR) practitioners use timelines to efficiently identify and better understand suspicious activity. The use of timelines has always been a core component of DFIR analysis (see Clifford Stoll's work in The Cuckoo's Egg), but over the last few years the importance of timelines has been increasingly highlighted in research [1], software [2] and training [3].

The foundations of timelines are obviously built on dates and times. We prefer timelines built on accurate dates and times, but consistently inaccurate dates and times, even in small clusters, may be extremely valuable. What happens to our timelines when we have reason to believe that critical dates and times from file systems, logs, embedded in documents, etc. cannot be trusted, not even to be consistently inaccurate?

We have confronted cases involving such widespread date and time tampering that the utility of "traditional" timeline analysis came into question. We realized that we had to dig deeper in these cases, and began formalizing our practice of identifying both legitimate and illegitimate anchors in relative time.

Let's break down the concept of identifying legitimate and illegitimate anchors in relative time. Legitimate and illegitimate anchors, ('anchors' are simply solid events we can rely on) are events that we can be confident are either legitimate or illegitimate, and upon which we can base additional analysis; sometimes without the benefit of accurate dates and times or, without any associated dates and times at all. Legitimate anchors used in the past have involved Microsoft's Windows operating system being installed, starting up, and shutting down.

Illegitimate anchors we have identified have involved the introduction of malware and anti-forensics tools (most often, data scrubbers) and/or remnants of their execution. "Relative time" refers to the time in which events happened in a certain order, but we cannot be certain the dates and times associated with those events; assuming that dates and times related to those events exist at all; are accurate. In fact, we are often certain that the dates and times related to these events are inaccurate.

The focus of this article is on anchors within your electronic evidence (i.e. internal anchors), but evidence does not exist in a vacuum; it exists in context with external anchors that might include court orders, video footage, historical events, etc. The designation of legitimate and illegitimate anchors should be guided and supported by what you know about the case and what you have learned about your evidence. Heavy doses of sanity checking are important here, e.g. leveraging dates and times within your evidence but from external sources (within remnants of web browsing, etc.). Also, in order to apply these anchors to relative time, we must be certain in what order they occurred and for that we can only rely on certain types of data which are not often exposed by digital forensics tools.

> ***"RELATIVE TIME REFERS TO THE TIME IN WHICH EVENTS HAPPENED IN A CERTAIN ORDER, BUT WE CANNOT BE CERTAIN THE DATES AND TIMES ASSOCIATED WITH THOSE EVENTS... ARE ACCURATE."***

/ TYPES OF ANCHORS IN RELATIVE TIME

Arsenal has found information produced by Microsoft's NTFS file system ("NTFS") and the Windows Event Log service particularly useful when determining the order in which events occurred, regardless of the dates and times associated with those events. This information includes:

- Log Sequence Numbers ("LSNs") from NTFS's $LogFile metafile ("$LogFile")
- Record numbers, which have not been re-used, from NTFS's $MFT metafile ("MFT")
- Record IDs (a.k.a. EventRecordIDs) from events created by the Windows Event Log service

The $LogFile is a transaction log that provides NTFS with redo and undo functionality by using unique identifiers called LSNs. In other words, the $LogFile keeps track of file system transactions so they can be redone, or undone, if necessary. LSNs increase sequentially (occurring in the order in which changes to files, folders, and their metadata happen) regardless of their associated dates and times. LSNs can be exposed by using tools such as Joakim Schicht's LogFile Parser [4] and G-C Partners Advanced NTFS Journal Parser [5].

The $MFT allows NTFS to keep track of its files and folders by maintaining information about their names, locations, dates and times, and much, much more. Each MFT record (in layman's terms, each file and folder) is assigned a record number as well as a sequence number that identifies whether that record has been re-used over time. When records have only been used once, i.e. their sequence number is "1", their record numbers increase sequentially, occurring in the order in which files and folders were created, regardless of their associated dates and times. $MFT record numbers and their sequence numbers can be exposed by using tools such as Joakim Schicht's mft2csv [6], the aforementioned G-C Partners Advanced NTFS Journal Parser, and David Kovar's analyzeMFT [7].

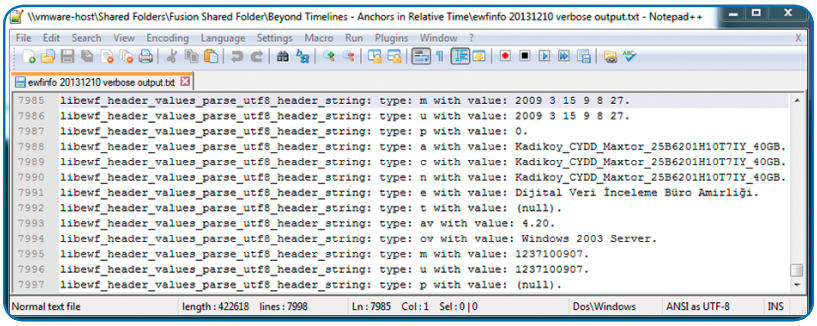


Figure 1. Windowshot – ewfinfo 20131210 – verbose output

Per Microsoft [8], "The Event Log service maintains a set of event logs that the system, system components, and applications use to record events." Record IDs are unique numbers assigned to events created by the Windows Event Log service and increase sequentially (occurring in the order in which events occurred) regardless of their associated dates and times. Record IDs can be exposed by using tools such as Harlan Carvey's, "lsevt.pl" Perl script.

/ APPLICATION OF ANCHORS IN RELATIVE TIME TO THE ERGENEKON CASE IN TURKEY

We have applied anchors in relative time to high-profile criminal cases in Turkey known as Sledgehammer, (specifically, against "Hard Drive No. 5" seized from the Turkish Naval Command on December 6, 2010) and Ergenekon. Sledgehammer involves the alleged planning of a Turkish military coup in response to the election of an Islamist political party (The Justice and Development Party a.k.a AKP). Ergenekon involves an alleged "deep state" [9] in Turkey with ties to the military, academia, NGOs, and the media. Spectators have referred to our findings, confirmed by digital forensics experts in the United States and abroad, as shocking and explosive.

Former executives of a Turkish non-governmental agency, Çagdas Yasamı Destekleme Dernegi (ÇYDD) are among the most controversial Ergenekon defendants. ÇYDD was founded in 1989 with a mission of protecting women's access to contemporary education. Prosecutors alleged that ÇYDD executives were recruiting new members into the terrorist organization Ergenekon, infiltrating the Turkish military, and laying the foundation for a coup.

The government's case against the ÇYDD executives is based largely on documents recovered from the "ÇYDD Hard Drive." The ÇYDD Hard Drive was seized (still inside its host computer) from ÇYDD's Kadıköy office by the Turkish police on April 13, 2009.

We received a copy of the forensic image obtained from the ÇYDD Hard Drive on August 5, 2013. Metadata within the forensic image indicated it was obtained March 15, 2009, which is not possible for reasons that include the ÇYDD Hard Drive having not been seized by that date. We found this fact (amongst others, more details will be available when the

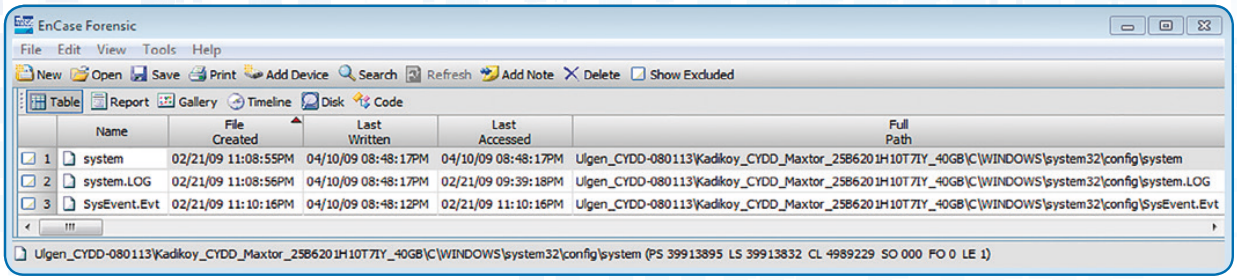


Figure 2. Windowshot – EnCase v6 – Windows Shutting Down

$LogFile Date/Time (SI)	$LogFile Action	Path	LSN
2009-04-10 20:48:12 (M)	UpdateResidentValue	...config\SysEvent.Evt	103773284
2009-04-10 20:48:17 (M)	UpdateResidentValue	...config\system	103782807
2009-04-10 20:48:17 (EM)	SetNewAttributeSizes	...config\system.LOG	103782964

Table 1. Windows Shutting Down

$LogFile Date/Time (SI)	$LogFile Action	Path	LSN
2009-03-17 18:15:41 (C)	InitializeFileRecordSegment	..._restore...4F39}	103816248
2009-03-17 18:15:41 (C)	InitializeFileRecordSegment	..._restore...4F39}\RP46	103816504
2009-03-22 09:31:46 (C)	InitializeFileRecordSegment	...4F39}\RP46\change.log	103816648

Table 2. Creation of Foreign Restore Point

$LogFile Date/Time (SI)	$LogFile Action	Path	LSN
2008-12-07 13:39:22 (C)	InitializeFileRecordSegment	...Türkan SAYLAN 3.doc	105364977
2008-12-25 23:42:23 (C)	InitializeFileRecordSegment	...MEKTUP(Türkan SAYLAN).doc	105385237
2008-12-30 11:48:08 (C)	InitializeFileRecordSegment	...liste açıklma.docx	105734328

Table 3. Creation of Critical Documents Cited by Prosecution

$LogFile Date/Time (SI)	$LogFile Action	Path	LSN
N/A	DeallocateFileRecordSegment	...liste açıklma.docx	106290462
N/A	DeallocateFileRecordSegment	...Türkan SAYLAN 3.doc	106306537
N/A	DeallocateFileRecordSegment	...MEKTUP(Türkan SAYLAN).doc	106307207

Table 4. Deletion of Critical Documents Cited by Prosecution

Event	Date/Time	LSN(s)
ÇYDD Hard Drive's Windows last shut down	2009-04-10 20:48:17	103782964
Turkish police raid ÇYDD Kadıköy	2009-04-13 09:30:00	N/A
Creation of foreign restore point	Forged	103816248
Creation of all documents cited by prosecution	Forged	104876939 – 106145854
Deletion of all documents cited by prosecution	Forged	106284798 – 106388914
Turkish police raid ÇYDD Kadıköy	2009-04-13 09:30:00	N/A
ÇYDD Hard Drive forensically imaged	Suspicious	N/A

Table 5. Event Sequence With Internal & External Anchors

TABLES KEY

The following key is associated with the tables in this article:

M = Modified
EM = Entry Modified
C = Created
SI = Standard Information

movie documenting our work is released) suspicious and began searching the ÇYDD Hard Drive for legitimate and illegitimate anchors in relative time.

In this case, we focused our efforts on file system transactions recorded in the $LogFile to identify both legitimate and illegitimate anchors. We determined that a legitimate anchor (LSN 103782964) involved Windows on the ÇYDD Hard Drive being shut down, for the last time, on Friday April 10, 2009 at approximately 8:48:17 PM (note: dates and times related to our findings mentioned in this article are in Turkish time). We used events created by the Windows Event Log service (e.g. Last Event Log service shutdown (event ID 6006) = 2009-04-10 20:48:12) and Registry (e.g. "ShutdownTime" at system\ControlSet001\Control\Windows = 2009-04-10 20:48:17) values to further solidify the selection of this anchor.

The LSNs in Table 1 are extremely important – they represent the last legitimate file system transactions that occurred on the ÇYDD Hard Drive. In other words, these events represent the "final acts" of Windows as it was shutting down and writing to critical system files.

As mentioned earlier, in some cases illegitimate anchors might involve malware or anti forensics. In this case, an illegitimate anchor in the $LogFile was quite obvious. Pay close attention

"SLEDGEHAMMER INVOLVES THE ALLEGED PLANNING OF A TURKISH MILITARY COUP IN RESPONSE TO THE ELECTION OF AN ISLAMIST POLITICAL PARTY."

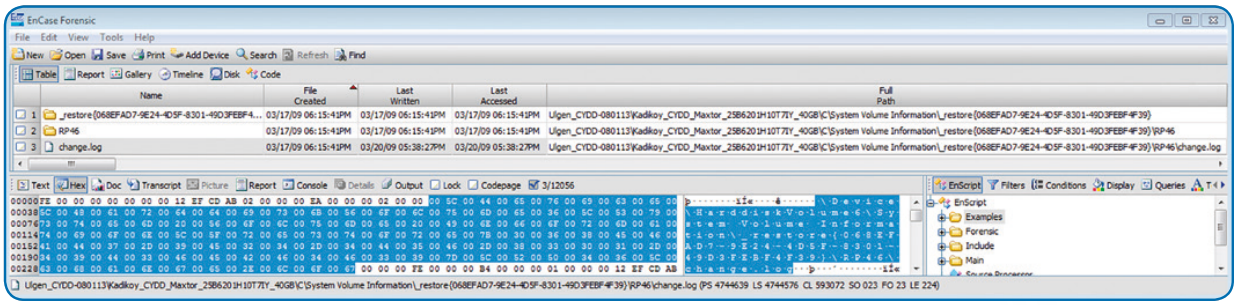


Figure 3. Windowshot – EnCase v6 – Foreign Restore Point

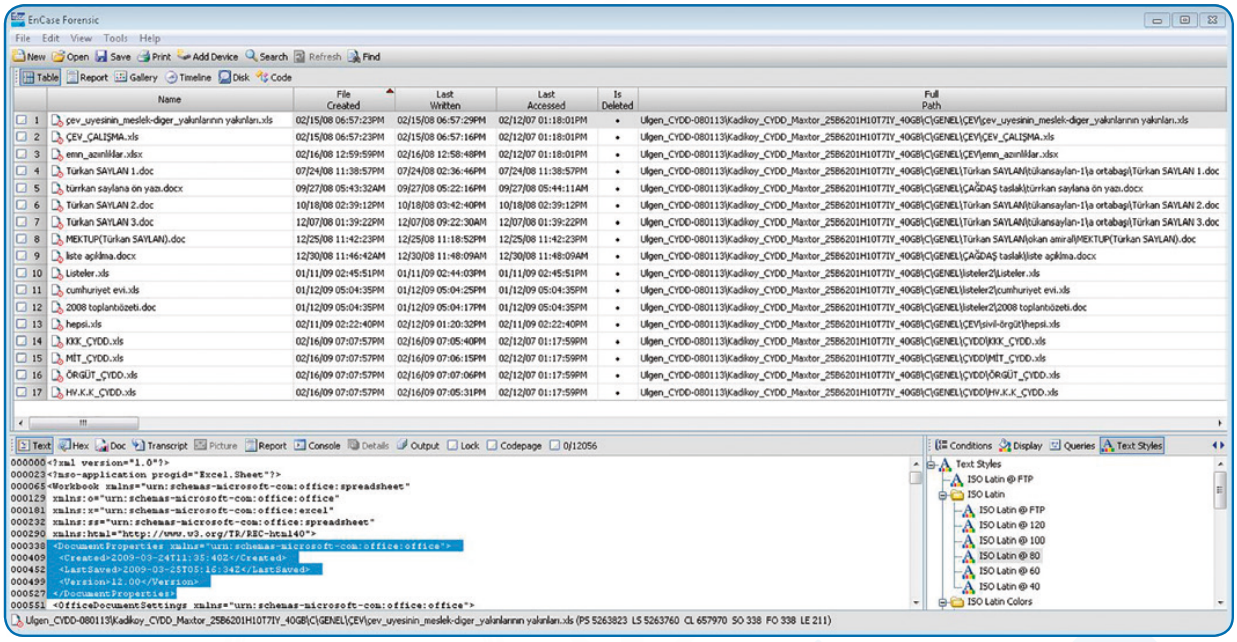


Figure 4. Critical Documents MAC Times

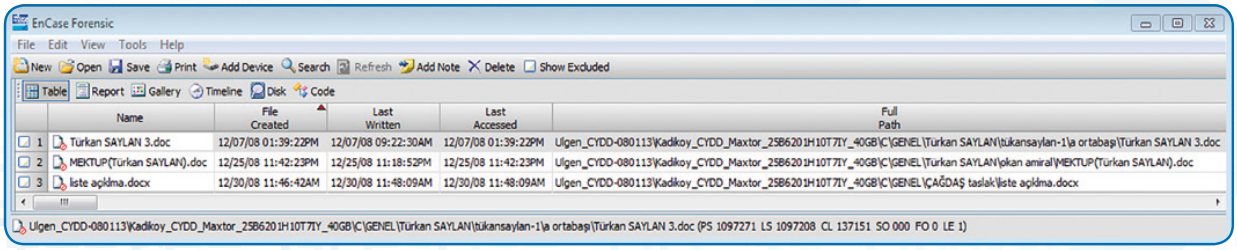


Figure 5. Windowshot – EnCase v6 – The 3

to the LSNs in Table 2, and compare them to the LSNs in Table 1. Keep in mind that LSNs increase sequentially, regardless of their associated dates and times, and the LSNs in Table 1 represent the last time that Windows was shut down on the ÇYDD Hard Drive.

The file system transactions in Table 2 (starting with LSN 103816248) represent the creation of a foreign restore point, as their LSNs are higher than those related to when Windows on the ÇYDD Hard Drive was last shut down in Table 1. In other words, a restore point was created not by Windows on the ÇYDD Hard Drive that had already been shut down for the last time, but some other Windows OS that mounted the ÇYDD Hard Drive as its slave (a.k.a. auxiliary or secondary volume).

Perhaps most damning, the contents of this restore point's transaction log (change.log) refer to the ÇYDD Hard Drive

as “HarddiskVolume6”, which Windows on the ÇYDD Hard Drive would not have done but another computer system running Windows would have. We confirmed this using Registry Recon to review “MountedDevices” and “Disk Devices” Registry information over time as well as searching the ÇYDD Hard Drive’s allocated and unallocated space.

Now that we have established an illegitimate anchor (LSN 103816248) related to the creation of a foreign restore point, let’s dig into the $LogFile more. There are 74,408 file system transactions (as parsed by LogFile Parser v1.0.0.16) from LSN 103816248 onward. All 74,408 transactions from LSN 103816248 onward are illegitimate as they occurred after Windows on the ÇYDD Hard Drive was shut down for the last time and after the ÇYDD Hard Drive was connected to another Windows system. Within these 74,408 transactions, every document cited in the government’s indictment of the ÇYDD executives is created and subsequently deleted. For example, arguably three of the most important documents in the government’s case against the ÇYDD defendants are created in Table 3. Again, pay close attention to the LSNs in Table 3 and how they relate to the LSNs in Tables 1 and 2.

These documents are critical to the government’s case because they establish the alleged connections between ÇYDD and Ergenekon. More specifically, “Türkan SAYLAN 3.doc” connects ÇYDD with retired Naval Colonel Aydın Ortabası and other active duty Naval officers indicted in Ergenekon, “MEKTUP(Türkan SAYLAN).doc” connects popular ÇYDD projects such as “Sea Star” (a ÇYDD program that selects university students to become societal leaders in particular subjects) to illegal activities and to Naval officers indicted in Ergenekon, and “liste açıklma.docx” connects female recipients of scholarships from ÇYDD with male students in Naval schools, purportedly to advance Ergenekon recruitment.

The ÇYDD Hard Drive presented us with an environment in which all dates and times had to be treated with extreme suspicion. Ultimately, it became clear that many of the most important dates and times could not be trusted. We leveraged legitimate and illegitimate anchors in relative time to identify the order in which important events occurred, determining that the ÇYDD Hard Drive had been tampered with. More detail regarding our findings related to $LogFile analysis on the ÇYDD Hard Drive will be made available at www.ArsenalExperts.com

When these anchors are put into context in Table 5 with case-related events (external anchors), in the order in which we now know they happened, their importance only increases. The only question we are left with in terms of the sequence of events, highlighted with grey colour coding, is whether the tampering occurred just before the raid or after it.

CONCLUSION

If our analysis of the ÇYDD Hard Drive had relied upon readily accessible dates and times, as others had done before us, we may have been misled by the evidence just as they were. Instead, we dug deeper by leveraging legitimate and illegitimate anchors in relative time to uncover evidence tampering, the ramifications of which are still not fully understood. What is quite clear, however, is that all is not lost when dates and times related to electronic evidence are hopelessly unreliable. If you identify the types of anchors mentioned in this article, you will gain an understanding of the order in which events happened regardless of what the dates and times associated with them would lead you to believe.

“IF YOU IDENTIFY THE TYPES OF ANCHORS MENTIONED IN THIS ARTICLE, YOU WILL GAIN AN UNDERSTANDING OF THE ORDER IN WHICH EVENTS HAPPENED REGARDLESS OF WHAT THE DATES AND TIMES ASSOCIATED WITH THEM WOULD LEAD YOU TO BELIEVE.”

REFERENCES

1. Mastering the Super Timeline With log2timeline, Kristinn Guojónsson, June 29, 2010
2. Plaso (http://plaso.kiddaland.net/), 4n6time (http://log2timeline.kiddaland.net/usage/4n6time)
3. SANS FOR508.3: Timeline Analysis (Advanced Computer Forensic Analysis and Incident Response)
4. https://code.google.com/p/mft2csv/wiki/LogFileParser
5. http://hackingexposedcomputerforensicsblog.blogspot.com/
6. https://code.google.com/p/mft2csv/
7. https://github.com/dkovar/analyzeMFT
8. http://technet.microsoft.com/en-us/library/dd315601(v=ws.10).aspx
9. http://en.wikipedia.org/wiki/Deep_state

AUTHOR BIOGRAPHY

Mark Spencer is President of Arsenal Consulting, where he leads engagements involving digital forensics for law firms, corporations, and government agencies. He is also President of Arsenal Recon, where he guides development of digital forensics tools. Mark has more than fifteen years of law-enforcement and private-sector digital forensics experience. He has taught at both the Computer Security Institute and Bunker Hill Community College in Boston. Mark has led the Arsenal team on many high-profile and high-stakes cases, from allegations of intellectual property theft and evidence spoliation to support of foreign terrorist organizations and military coup planning. Arsenal Consulting and Recon are located in the Chelsea Naval Magazine, a historic military structure which once stored arms for the USS Constitution, just outside Boston, Massachusetts.

Arsenal Consulting

— ARM YOURSELF —

COMPUTER FORENSICS
IN BOSTON AND BEYOND

INTELLECTUAL PROPERTY THEFT, EVIDENCE SPOLIATION, INTERNET INVESTIGATIONS, FINANCIAL FRAUD, COMPUTER INTRUSION, EXTORTION

THE ARSENAL DIFFERENCE

Do you know where your electronic evidence is?
Without computer forensics, you don't. Whether you are involved in an internal investigation or ongoing litigation, traditional electronic discovery only scratches the surface when it comes to locating and understanding critical electronic data. Arsenal clients have repeatedly found that utilizing computer forensics provides them with improved insight into internal matters and a significant advantage when it comes to ongoing disputes.

Team
The Arsenal team is led by President Mark Spencer, who has over fifteen years of law-enforcement and private-sector computer forensics experience. We are forensic practitioners at our core and not your typical "computer guys." When faced with adversity, our personnel don't give up - they fight harder.

Approach
Arsenal specializes in applying the most powerful computer forensics tools and techniques to provide consulting services in high-profile and high-stakes cases. Our services, using methods acceptable in courts of law, result in clear and concise answers for our clients.

Experience
We have extensive experience with both criminal and civil litigation, having served as expert consultants and witnesses in state, federal, and international courts. Our hard-fought experience allows us to better understand clients' challenges and tailor the best solutions for them. In addition to providing consulting services, we develop computer forensics tools and train our peers.

"It is Arsenal's curiosity and tenacity that sets them apart. On every case Arsenal has worked on for us, they have managed to locate smoking gun evidence in a variety of places."

— Mark Whitney, Attorney
Morgan, Brown & Joy, LLP

"I have worked with computer forensics teams on numerous white-collar matters in the past, and Mark Spencer and his team at Arsenal were unquestionably the best I have seen."

— Sejal Patel, Attorney
Law Office of Sejal Patel, LLC

"I have terrific technical sources all around the world by now, including in the CIA and the FBI, but when I need help dealing with computer forensics and cyber-crime, I always turn first to Mark Spencer."

— Joseph Finder, New York Times bestselling author of Vanished, Paranoia, and High Crimes

www.ArsenalExperts.com

285 Commandants Way, Chelsea, Massachusetts 02150 | Phone: 617-ARSENAL (277-3625) Fax: 617-934-4298 | Email: info@ArsenalExperts.com