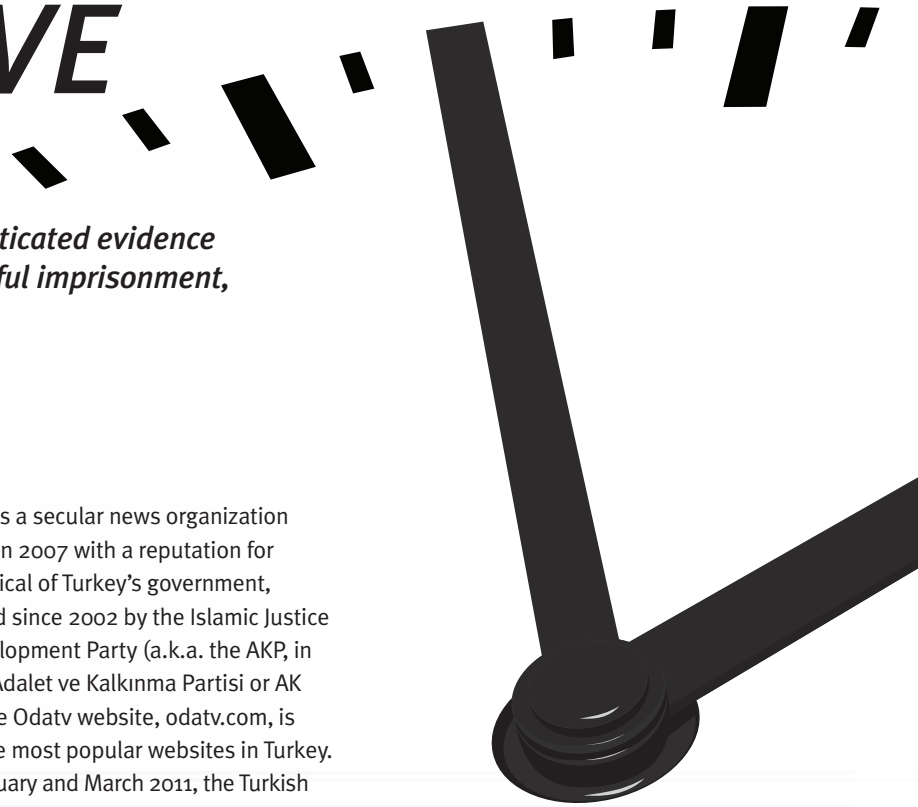
APPLYING ANCHORS IN RELATIVE TIME



Our most powerful weapon reveals sophisticated evidence tampering which led to journalists' wrongful imprisonment, explains Mark Spencer...

/ INTERMEDIATE

Everyone said it was the malware. Everyone, including digital forensics experts at universities and consulting companies in the United States and abroad, was wrong. The failure of so many experts to identify an unprecedented series of electronic attacks against journalists, the likes of which we may never see again, almost resulted in the fascinating truth being buried forever.

"Anchors in Relative Time" ("ART") is an analysis technique described in my article "Beyond Timelines – Anchors in Relative Time" published in *Digital Forensics Magazine* Issue 18. As a quick summary, this technique involves identifying legitimate and illegitimate anchors within electronic evidence that can be placed in relative time (time in which events have happened in a certain order) regardless of whether dates and times associated with those anchors are accurate. My last article focused on three particular types of anchors found on Microsoft Windows ("Windows") systems to which I now add a couple more as highlighted in Table 1.

These types of anchors are particularly useful when determining the order in which events have occurred, regardless of any associated dates and times, as they normally increment in the order events have occurred. See the Definitions section at the end of this article for more details on each anchor type and source. Important events in our cases have included Windows starting up and shutting down, malware introduction and execution, and critical documents being created and deleted.

Odatv is a secular news organization founded in 2007 with a reputation for being critical of Turkey's government, controlled since 2002 by the Islamic Justice and Development Party (a.k.a. the AKP, in Turkish, Adalet ve Kalkınma Partisi or AK Parti). The Odatv website, odatv.com, is one of the most popular websites in Turkey.

In February and March 2011, the Turkish National Police began a series of raids and arrests involving Odatv. Critical electronic evidence seized during the raids appeared to connect Odatv employees and supporters to the Ergenekon terrorist organization. In November 2011, an indictment in essence charged Odatv with being the media wing of Ergenekon and singled out 14 Odatv employees and supporters. The indictment was based on electronic documents seized during the raids by the Turkish National Police, leading to the imprisonment of 11 of the 14 suspects.

Barış Pehlivan, whose Odatv computer is the focus of this article, is a well-known investigative journalist, editor, producer and author, who worked at Odatv since its 2007 origin. He was among those arrested in February 2011, and was imprisoned for a year and a half (February 14, 2011 – September 14, 2012) based on documents recovered from

/ ERGENEKON

Ergenekon is an alleged secularist "deep state" in Turkey with ties to the military, academia, NGOs, and the media. Ergenekon members were charged with plotting to overthrow the Turkish government in a series of 15 indictments between 2008 and 2011.

/ SLEDGEHAMMER

Sledgehammer involves the alleged planning of a Turkish military coup in response to the election of the AKP. Forged documents critical to the Sledgehammer trial include purported plans to bomb mosques, shoot down a fighter jet, and ultimately overthrow the Turkish government. ART analysis revealed the true nature of the forged documents.

Anchor Type	Anchor Source
Log Sequence Numbers ("LSNs")	NTFS $LogFile
Record Numbers (Sequence Number 1s)	NTFS $MFT
SecurityIds	NTFS $Secure
Update Sequence Numbers ("USNs")	NTFS $UsnJrnl
RecordNumbers or EventRecordIDs	Event Logging or Windows Event Log

Table 1. Anchor Summary

RecordNumber	Event Number	Event Description	Date/Time (UTC)
28202	6005	Event Log Service Start	02/09/2011 07:44:03
28229	6006	Event Log Service Stop	02/09/2011 17:58:46
28231	6005	Event Log Service Start	02/09/2011 20:09:14
28250	6006	Event Log Service Stop	02/09/2011 20:10:13
28252	6005	Event Log Service Start	02/10/2011 08:05:42
28295	6006	Event Log Service Stop	02/10/2011 18:03:32
28297	6005	Event Log Service Start	02/11/2011 07:39:13
28321	6006	Event Log Service Stop	02/11/2011 17:18:31
28323	6005	Event Log Service Start	02/11/2011 20:54:13
28343	6006	Event Log Service Stop	02/11/2011 20:55:16

Table 2. Partition 1 – System Event Log – Windows Start/Stops

Light Blue = Event Log Service Start
Dark Blue = Event Log Service Stop

both his Odatv and personal computers. As you will soon learn, those documents were not quite what they seemed.

We at Arsenal have extensive experience uncovering evidence spoliation and are particularly sceptical of any evidence related to Ergenekon and other high-profile Turkish trials, such as Sledgehammer.

The presence of malware on Odatv-related computers (Barıs Pehlivan's Odatv and personal computers, Müyesser Yıldız's personal computer) has been documented in a cursory way in many technical reports. While malware was in fact found on Mr. Pehlivan's Odatv Computer, it was readily apparent after applying ART that malware was not responsible for the creation and deletion of the incriminating documents.

/ WINDOWS STARTUPS AND SHUTDOWNS PER EVENT LOG SERVICE

To become properly oriented with a piece of evidence using ART it is often useful to identify "legitimate" anchors involving Windows startups and shutdowns. Identifying these anchors on Windows boot volumes is relatively straightforward, but identifying them on auxiliary volumes can be quite challenging. Why then deal with the frustration of identifying these anchors not only on Windows boot volumes but also on auxiliary volumes? Generally speaking, operating in the initial fog of suspected evidence tampering demands anchors on every volume that can be relied upon, even if their associated dates and times cannot be trusted. More specifically, suspicious activity was found on both volumes of Mr. Pehlivan's Odatv computer and these anchors proved to be critical to understanding what actually happened to them.

In order to identify anchors reflecting Windows startups and shutdowns on Mr. Pehlivan's Odatv computer (on both the Windows boot and auxiliary volumes) we used a combination of Event Log service events and file system transactions.

Starting with the Event Log service, we identified startups and shutdowns of that particular service, which are normally consistent with Windows startups and shutdowns. We attained a high level of comfort with the values in Table 2 as legitimate anchors by looking for signs of tampering (e.g., inconsistencies between date/times and the normal progression of RecordNumbers) which would have affected the Event Logs (finding none), reviewing Event Log service startups and shutdowns over time, comparing these events to file system transactions discussed in this article, and considering what we know from external anchors such as the normal behaviour of Odatv employees.

While we were comfortable that the anchors from February 9, 2011 onward mentioned in Table 2 were legitimate (their dates and times were consistent with "real time", i.e., their dates and times could be relied upon) we found RecordNumbers 28231/28250 and 28323/28343 unusual based on our review of Event Log service startups and shutdowns over time as well as our understanding of the normal behaviour of Odatv employees.

> *"THE FAILURE OF SO MANY EXPERTS TO IDENTIFY AN UNPRECEDENTED SERIES OF ELECTRONIC ATTACKS AGAINST JOURNALISTS, THE LIKES OF WHICH WE MAY NEVER SEE AGAIN, ALMOST RESULTED IN THE FASCINATING TRUTH BEING BURIED FOREVER."*

/ WINDOWS STARTUPS AND SHUTDOWNS PER FILE SYSTEM TRANSACTIONS ON FIRST PARTITION

Next, we identified file system transactions in the NTFS $UsnJrnl and $LogFile metafiles which uniquely identified Windows startups and shutdowns.

After modelling Windows startups and shutdowns on the Windows boot volume (the first partition) of Mr. Pehlivan's Odatv computer over time, we found that $UsnJrnl transactions "DATA_TRUNCATION" and "CLOSE+DATA_EXTEND+DATA_TRUNCATION+SECURITY_CHANGE" involving pagefile.sys uniquely and consistently identified Windows startups and shutdowns. See Table 3 for a list of those transactions from February 9, 2011 onward.

USN Number	Filename	Reason	Date/Time (UTC)
11727337976	pagefile.sys	DATA_TRUNCATION	02/09/2011 07:43:55.859
11755837856	pagefile.sys	CLOSE+DATA_EXTEND+DATA_ TRUNCATION+SECURITY_CHANGE	02/09/2011 17:58:56.953
11755847496	pagefile.sys	DATA_TRUNCATION	02/09/2011 20:09:06.921
11755922248	pagefile.sys	CLOSE+DATA_EXTEND+DATA_ TRUNCATION+SECURITY_CHANGE	02/09/2011 20:10:21.156
11755922600	pagefile.sys	DATA_TRUNCATION	02/10/2011 08:05:34.937
11783809040	pagefile.sys	CLOSE+DATA_EXTEND+DATA_ TRUNCATION+SECURITY_CHANGE	02/10/2011 18:03:42.187
11783809216	pagefile.sys	DATA_TRUNCATION	02/11/2011 07:39:05.140
11805428080	pagefile.sys	CLOSE+DATA_EXTEND+DATA_ TRUNCATION+SECURITY_CHANGE	02/11/2011 17:18:45.843
11805432752	pagefile.sys	DATA_TRUNCATION	02/11/2011 20:54:06.171

Table 3. Partition 1 – $UsnJrnl – Windows Start/Stops

Light Blue = Windows Start
Dark Blue = Windows Stop

LSN Number	Related USN	Filename	Reason	Date/Time (UTC)*
68357995732	11805428080	pagefile.sys	UpdateNonResidentValue	02/11/2011 17:18:45.843
68358125595	11805432752	pagefile.sys	UpdateNonResidentValue	02/11/2011 20:54:06.171

Table 4. Partition 1 – $LogFile – USN Windows Start/Stop Associations

*$UsnJrnl timestamps within $LogFile

Light Blue = Windows Start
Dark Blue = Windows Stop

LSN Number	File or Folder Name	Reason	Date/Time (UTC)*
626857812	System Volume Information	UpdateResidentValue	02/09/2011 07:44:01.343
626857914	$Reparse	UpdateResidentValue	02/09/2011 07:44:01.375
627014061	tracking.log	UpdateResidentValue	02/09/2011 17:58:50.343
627014084	System Volume Information	UpdateFileNameAllocation	02/09/2011 17:58:50.343
637786268	System Volume Information	UpdateResidentValue	02/09/2011 20:09:12.406
637786370	$Reparse	UpdateResidentValue	02/09/2011 20:09:12.437
637787707	tracking.log	UpdateResidentValue	02/09/2011 20:10:13.640
637787748	System Volume Information	UpdateFileNameAllocation	02/09/2011 20:10:13.640
637788225	System Volume Information	UpdateResidentValue	02/10/2011 08:05:40.421
637788327	$Reparse	UpdateResidentValue	02/10/2011 08:05:40.421
637821309	tracking.log	UpdateResidentValue	02/10/2011 18:03:37.265
637821332	System Volume Information	UpdateFileNameAllocation	02/10/2011 18:03:37.265
637821713	System Volume Information	UpdateResidentValue	02/11/2011 07:39:10.718
637821815	$Reparse	UpdateResidentValue	02/11/2011 07:39:10.750
637856797	tracking.log	UpdateResidentValue	02/11/2011 17:18:37.046
637856820	System Volume Information	UpdateFileNameAllocation	02/11/2011 17:18:37.046
638168609	System Volume Information	UpdateResidentValue	02/11/2011 20:54:11.609
638168711	$Reparse	UpdateResidentValue	02/11/2011 20:54:11.625
638169952	tracking.log	UpdateResidentValue	02/11/2011 20:55:16.328
638169993	System Volume Information	UpdateFileNameAllocation	02/11/2011 20:55:16.328

Table 5. Partition 2 – $LogFile – Windows Start/Stops

*Last Accessed (Standard Information Attribute)

Light Blue = Windows Start
Dark Blue = Windows Stop

"LEVERAGING ART MAY BE THE ONLY WAY OUT OF THE FOG WHEN ATTACKERS HAVE GONE TO GREAT LENGTHS TO DECEIVE YOU."

Two of the $UsnJrnl transactions in Table 3 (the last two) we can confirm by reviewing their associated $LogFile entries in Table 4.

Why can we only confirm two of the $UsnJrnl transactions in the $LogFile? On a typical Windows boot volume, the $UsnJrnl transactions go back much further in time than the more granular $LogFile. As expected, the $LogFile on the first partition of Mr. Pehlivan's Odatv computer, relatively speaking, did not go very far back in time.

/ WINDOWS STARTUPS AND SHUTDOWNS PER FILE SYSTEM TRANSACTIONS ON SECOND PARTITION

As mentioned above, identifying legitimate Windows startup and shutdown anchors on auxiliary (non-boot) volumes can be challenging. In the case of Mr. Pehlivan's Odatv computer, quite a bit of trial and error was required before finding combinations of $LogFile transactions which uniquely and consistently identified Windows startups and shutdowns on his computer. While it would be convenient if the combinations of events selected in this case applied to all non-boot Windows volumes, we already know from testing that they do not. When considering anchors relied on for ART, particularly anchors related to non-boot volumes, it is best to treat each Windows system as unique and model file system behaviour anew.

The logical question arises: which combinations of $LogFile transactions did we use to uniquely and consistently identify Windows startup and shutdown on the auxiliary volume, the second partition, of Mr. Pehlivan's Odatv computer?
We found that UpdateResidentValue transactions, in rapid succession and involving the $Reparse metafile and System Volume Information folder, were solid anchors for his Windows startups.
We then found that UpdateResidentValue transactions involving tracking.log, in rapid succession with UpdateFileNameAllocation transactions involving the System Volume Information folder, were solid anchors for his Windows shutdowns.

Table 5 contains the $LogFile transactions from the second partition of Mr. Pehlivan's Odatv computer we used to uniquely identify Windows startup and shutdown from February 9, 2011 onward.

Why did we rely on $UsnJrnl transactions on the first partition and $LogFile transactions on the second for our anchors? The $LogFile on the first partition did not go very far back in time and the second did not have the $UsnJrnl enabled (Windows does not enable the change journal on auxiliary volumes by default).

Tables 6 and 7 summarize Windows startup and shutdown anchors on each partition. These anchors allow us to put important events whose dates and times have been forged into context with Windows startups and shutdowns whose dates and times are accurate.

/ SUSPICIOUS ACTIVITY ON SECOND PARTITION

Odatv's defense team advised Arsenal that there were 11 critical documents used by the prosecution, all of which were found in a deleted state on the second partition of Mr. Pehlivan's Odatv computer. Table 8 puts the creation and deletion of these documents into context with Windows startups and shutdowns.

So, armed with insight from Table 8 into suspicious activity involving the second partition of Mr. Pehlivan's Odatv computer, you well may have some eyebrow-raising questions. Also, keeping in mind these documents formed the basis for imprisoning Barıs Pehlivan for 18 months, they are compelling questions indeed:

- How were these critical documents created and deleted on the hard drive the evenings of February 9 and 11, when its Windows was not running?
- Why were their dates and times forged?
- Why were they deleted just after they were created?
- Why was Windows briefly booted each evening after the creations and deletions?
- What kinds of documents could be so potent as to result in the imprisonment of Barıs Pehlivan and 10 other Odatv journalists and supporters?

Anchor #	Anchor Type	Start/Stop	Date/Time (UTC)
11727337976	$UsnJrnl	Start	02/09/2011 07:43:55.859
11755837856	$UsnJrnl	Stop	02/09/2011 17:58:56.953
11755847496	$UsnJrnl	Start	02/09/2011 20:09:06.921
11755922248	$UsnJrnl	Stop	02/09/2011 20:10:21.156
11755922600	$UsnJrnl	Start	02/10/2011 08:05:34.937
11783809040	$UsnJrnl	Stop	02/10/2011 18:03:42.187
11783809216	$UsnJrnl	Start	02/11/2011 07:39:05.140
11805428080	$UsnJrnl	Stop	02/11/2011 17:18:45.843
11805432752	$UsnJrnl	Start	02/11/2011 20:54:06.171

Table 6. Partition 1 – Windows Start/Stops

Light Blue = Windows Start
Dark Blue = Windows Stop

Anchor #	Anchor Type	Start/Stop	Date/Time (UTC)*
626857812	$LogFile	Start	02/09/2011 07:44:01.343
627014084	$LogFile	Stop	02/09/2011 17:58:50.343
637786268	$LogFile	Start	02/09/2011 20:09:12.406
637787748	$LogFile	Stop	02/09/2011 20:10:13.640
637788225	$LogFile	Start	02/10/2011 08:05:40.421
637821332	$LogFile	Stop	02/10/2011 18:03:37.265
637821713	$LogFile	Start	02/11/2011 07:39:10.718
637856820	$LogFile	Stop	02/11/2011 17:18:37.046
638168609	$LogFile	Start	02/11/2011 20:54:11.609
638169993	$LogFile	Stop	02/11/2011 20:55:16.328

Table 7. Partition 2 – Windows Start/Stops

Light Blue = Windows Start
Dark Blue = Windows Stop

*Last Accessed (Standard Information Attribute)

Anchor #	Anchor Type	Event	Event Detail	Date/Time (UTC)*
626857812	$LogFile	Windows Start	UpdateResidentValue	02/09/2011 07:44:01.343
627014084	$LogFile	Windows Stop	UpdateFileNameAllocation	02/09/2011 17:58:50.343
637682398	$LogFile	Document Creation	SY.doc	11/11/2010 15:42:31.171
637682875	$LogFile	Document Creation	Yalçın hoca.doc	11/11/2010 15:42:31.171
637690961	$LogFile	Document Deletion	SY.doc	N/A
637691149	$LogFile	Document Deletion	Yalçın hoca.doc	N/A
637786268	$LogFile	Windows Start	UpdateResidentValue	02/09/2011 20:09:12.406
637787748	$LogFile	Windows Stop	UpdateFileNameAllocation	02/09/2011 20:10:13.640
637788225	$LogFile	Windows Start	UpdateResidentValue	02/10/2011 08:05:40.421
637821332	$LogFile	Windows Stop	UpdateFileNameAllocation	02/10/2011 18:03:37.265
637821713	$LogFile	Windows Start	UpdateResidentValue	02/11/2011 07:39:10.718
637856820	$LogFile	Windows Stop	UpdateFileNameAllocation	02/11/2011 17:18:37.046
637868334	$LogFile	Document Creation	toplantı.doc	04/26/2010 08:36:39.140
637877980	$LogFile	Document Creation	teRTEmiz.doc	07/26/2010 09:55:57.500
637878444	$LogFile	Document Creation	Bilinçlendirme.doc	07/26/2010 09:55:57.546
637878963	$LogFile	Document Creation	Hanefi.doc	07/26/2010 09:55:57.546
637891763	$LogFile	Document Creation	Koz.doc	08/16/2010 10:32:20.031
637892214	$LogFile	Document Creation	Nedim.doc	08/16/2010 10:32:20.046
637908831	$LogFile	Document Creation	Ulusal Medya 2010.doc	09/28/2010 11:54:42.593
638067782	$LogFile	Document Creation	Sabri Uzun.doc	12/20/2010 09:46:21.609
638077281	$LogFile	Document Creation	Org mu.doc	01/11/2011 09:24:29.921
638081144	$LogFile	Document Deletion	Org mu.doc	N/A
638083419	$LogFile	Document Deletion	Ulusal Medya 2010.doc	N/A
638138698	$LogFile	Document Deletion	Koz.doc	N/A
638138860	$LogFile	Document Deletion	Nedim.doc	N/A
638139034	$LogFile	Document Deletion	Sabri Uzun.doc	N/A
638153158	$LogFile	Document Deletion	Hanefi.doc	N/A
638153441	$LogFile	Document Deletion	teRTEmiz.doc	N/A
638153578	$LogFile	Document Deletion	Bilinçlendirme.doc	N/A
638157265	$LogFile	Document Deletion	toplantı.doc	N/A
638168609	$LogFile	Windows Start	UpdateResidentValue	02/11/2011 20:54:11.609
638169993	$LogFile	Windows Stop	UpdateFileNameAllocation	02/11/2011 20:55:16.328

Table 8. Partition 2 – $LogFile – Critical Documents Creation/Deletion

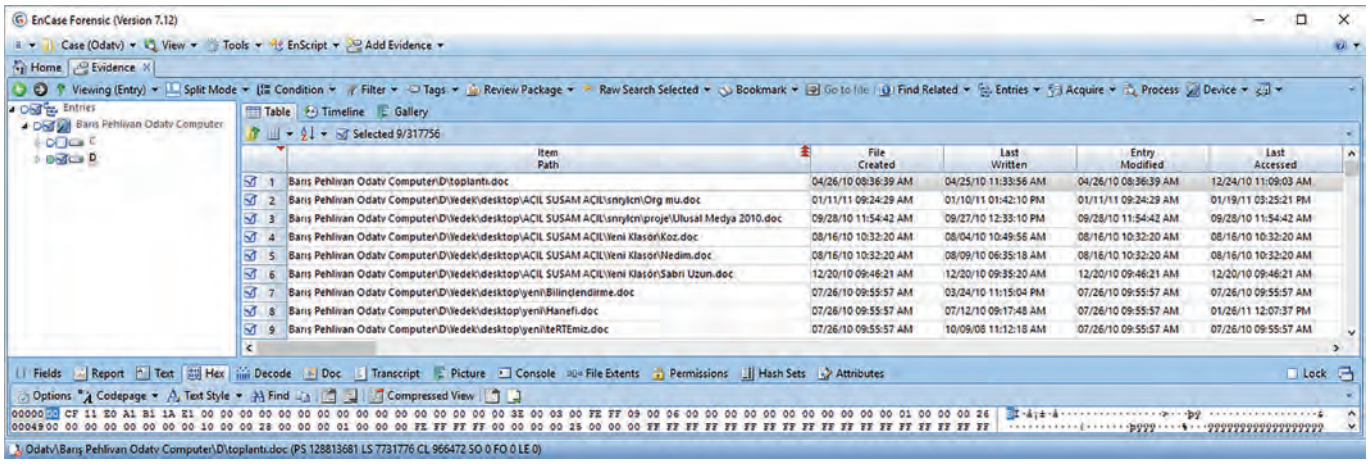
* Windows Start/Stop = Last Accessed (Standard Information Attribute) / Document Creation = MFT Entry Modified (Filename Information Attribute)

Light Blue = Windows Start
Dark Blue = Windows Stop
Grey = Suspicious Event

Anchor #	Anchor Type	Event	Event Detail	Date/Time (UTC)
11727337976	$UsnJrnl	Windows Start	DATA_TRUNCATION	02/09/2011 07:43:55.859
11755837856	$UsnJrnl	Windows Stop	CLOSE+DATA_EXTEND+DATA_TRUNCATION+SECURITY_CHANGE	02/09/2011 17:58:56.953
11755844512	$UsnJrnl	RAT Creation	...Administrator\Start Menu...\MSN Messenger.exe...	01/19/2011 14:08:33.875
11755845600	$UsnJrnl	RAT Creation	...Türker\Start Menu...\MSN Messenger.exe...	01/19/2011 14:08:59.000
11755846272	$UsnJrnl	RAT Creation	...All Users\Start Menu...\MSN Messenger...	01/19/2011 14:09:24.609
11755847496	$UsnJrnl	Windows Start	DATA_TRUNCATION	02/09/2011 20:09:06.921
11755922248	$UsnJrnl	Windows Stop	CLOSE+DATA_EXTEND+DATA_TRUNCATION+SECURITY_CHANGE	02/09/2011 20:10:21.156
11755922600	$UsnJrnl	Windows Start	DATA_TRUNCATION	02/10/2011 08:05:34.937
11783809040	$UsnJrnl	Windows Stop	CLOSE+DATA_EXTEND+DATA_TRUNCATION+SECURITY_CHANGE	02/10/2011 18:03:42.187
11783809216	$UsnJrnl	Windows Start	DATA_TRUNCATION	02/11/2011 07:39:05.140
11805428080	$UsnJrnl	Windows Stop	CLOSE+DATA_EXTEND+DATA_TRUNCATION+SECURITY_CHANGE	02/11/2011 17:18:45.843
11805431432	$UsnJrnl	RAT Creation	...Administrator\Start Menu...\windows.exe...	12/24/2010 11:10:56.000
11805431960	$UsnJrnl	RAT Creation	...Türker\Start Menu...\windows.exe...	12/24/2010 11:11:20.015
11805432752	$UsnJrnl	Windows Start	DATA_TRUNCATION	02/11/2011 20:54:06.171

Table 9. Partition 1 – $UsnJrnl – RAT Creation/Deletion

Light Blue = Windows Start
Dark Blue = Windows Stop
Grey = Suspicious Event



Critical documents created & deleted February 11, 2011 as seen by Guidance Software's EnCase

Let's answer the final question now to provide important context; the documents appeared to reveal members of Ergenekon shaping Odatv policy to attack the government and Gülenist movement (a religious and social movement led by Turkish Islamic scholar and preacher Fethullah Gülen), with particular emphases on the Ergenekon and Sledgehammer trials.

It should be noted that at this stage of our analysis, we saw distinct and troubling similarities between Mr. Pehlivan's Odatv computer and critical Ergenekon evidence seized from the Turkish Naval Command and the non-governmental organization Çagdas Yasamı Destekleme Dernegi – see "Beyond Timelines – Anchors in Relative Time" published in *Digital Forensics Magazine* Issue 18 for more detail.

/ SUSPICIOUS ACTIVITY ON FIRST PARTITION

Now that we have discussed the second partition of Mr. Pehlivan's Odatv computer, what was happening to the first partition during these suspicious times on February 9 and 11 when employees had normally departed? As seen in Table 9, we observed fascinating things happening.

Remote Access Trojans, or RATs, are malware applications designed to provide an attacker covert remote access to a computer system. Table 9 reflects the creation of RATs on Mr. Pehlivan's Odatv computer hard drive during the evenings of February 9 and 11, when its Windows was not running. The RAT installed the evening of February 9, Bandook (developed by Nuclear Winter Crew a.k.a Prince Ali or Ali Khachab, with interesting functionality including persistence, firewall bypass, plugins, and more), is quite familiar to Arsenal. The RAT installed the evening of February 11 is a different animal entirely.

At this point in our analysis, we had reason to believe that Mr. Pehlivan's Odatv computer hard drive was attacked locally during the evenings of February 9 and 11. Each of these local attacks involved:

- Removing Mr. Pehlivan's Odatv computer hard drive
- Connecting the hard drive to a "foreign" computer system (which, among other things, allowed for relatively sophisticated date and time tampering)
- Copying incriminating documents to the hard drive from the foreign computer
- Deleting the incriminating documents on the hard drive
- Copying RATs to the hard drive
- Reinstalling the hard drive in Mr. Pehlivan's Odatv computer
- Briefly rebooting and logging into Mr. Pehlivan's Odatv computer (which would confirm that the attackers reinstalled the hard drive properly and executed the RATs* so they could manipulate his computer remotely)

* In theory at least – Bandook did not actually execute and "drop" until a login the following morning

/ HUNTING THE AHTAPOT

The question is begged; if an attacker copied incriminating documents and a RAT to Mr. Pehlivan's Odatv computers hard drive the evening of February 9, why risk another attack involving the removal of his hard drive the evening of February 11? The details of our RAT analysis are worthy of another article, but suffice to say we doubt the attackers had a choice, they had more documents to deliver but were apparently unable to establish a connection with the RAT they had installed on February 9.

Based on the attackers' previous failures (more on those soon), we believe that the RAT installed the evening of February 11 represented a "last resort." In other words, the attackers were desperate and willing to use methods and technology that they would have preferred to avoid. What technology might that be? Arsenal and Sophos Ltd., who will soon have more to say on the matter, call it "Ahtapot."

Ahtapot (Octopus in English) was copied to Mr. Pehlivan's Odatv computer hard drive the evening of February 11 and then executed when the attackers briefly booted the computer as their last act just prior to 11pm local time. Ahtapot appears to be a homegrown Turkish RAT, which has been used extremely sparingly. Some antivirus vendors, including Sophos Ltd., have never seen Ahtapot "in the wild." Arsenal worked with VirusShare.com to search over 24 million malware samples with fuzzy hashes and no Ahtapot hits were found. Ahtapot contains three components; "tohum", "beyin", and "kol" or in English "seed", "brain", and "arm." The seed is an installer, the brain provides the typical RAT-type functionality, and the arm is an injector which copies (or, injects) important strings into live memory. See Table 10 for hash values related to these three components. To characterize Ahtapot as "homegrown" is hardly to indicate that it was cobbled together haphazardly,

Date/Time (UTC)	Event	Event Detail	Anchor #	Anchor Type
02/09/2011 07:43:55.859	Windows Start	Typical Windows Start Time	11727337976	$UsnJrnl
02/09/2011 17:58:56.953	Windows Stop	Typical Windows Stop Time	11755837856	$UsnJrnl
Forged (Foreign Computer Attachment)	RAT Creation	Bandook RAT Created	11755844512-11755846272	$UsnJrnl
02/09/2011 20:09:06.921	Windows Start	Suspicious Windows Start Time	11755847496	$UsnJrnl
02/09/2011 20:10:21.156	Windows Stop	Suspicious Windows Stop Time	11755922248	$UsnJrnl
02/10/2011 08:05:34.937	Windows Start	Typical Windows Start Time	11755922600	$UsnJrnl
02/10/2011 08:07:56.703	RAT Execution	Bandook RAT Executed	11756050704	$UsnJrnl
02/10/2011 18:03:42.187	Windows Stop	Typical Windows Stop Time	11783809040	$UsnJrnl
02/11/2011 07:39:05.140	Windows Start	Typical Windows Start Time	11783809216	$UsnJrnl
02/11/2011 17:18:45.843	Windows Stop	Typical Windows Stop Time	11805428080	$UsnJrnl
Forged (Foreign Computer Attachment)	RAT Creation	Ahtapot RAT Created	11805431432-11805431960	$UsnJrnl
02/11/2011 20:54:06.171	Windows Start	Suspicious Windows Start Time	11805432752	$UsnJrnl
02/11/2011 20:54:28.156	RAT Execution	Ahtapot RAT Executed	11805453040	$UsnJrnl
02/11/2011 20:55:16	Windows Stop	Suspicious Windows Stop Time	28343	Event Log
02/14/2011 04:00:00 (Approximately)	Police Raid Odatv	Turkish National Police Raid Odatv	N/A	External

Table 11. Partition 1 – Suspicious Activity Summary

Light Blue = Windows Start
Dark Blue = Windows Stop
Grey = Suspicious Event

Date/Time (UTC)*	Event	Event Detail	Anchor #	Anchor Type
02/09/2011 07:44:01.343	Start	Typical Windows Start Time	626857812	$LogFile
02/09/2011 17:58:50.343	Stop	Typical Windows Stop Time	627014084	$LogFile
Forged (Foreign Computer Attachment)	Document Creation	Critical Documents Used By Prosecution	637682398-637682875	$LogFile
N/A (Foreign Computer Attachment)	Document Deletion	Critical Documents Used By Prosecution	637690961-637691149	$LogFile
02/09/2011 20:09:12.406	Start	Suspicious Windows Start Time	637786268	$LogFile
02/09/2011 20:10:13.640	Stop	Suspicious Windows Stop Time	637787748	$LogFile
02/10/2011 08:05:40.421	Start	Typical Windows Start Time	637788225	$LogFile
02/10/2011 18:03:37.265	Stop	Typical Windows Stop Time	637821332	$LogFile
02/11/2011 07:39:10.718	Start	Typical Windows Start Time	637821713	$LogFile
02/11/2011 17:18:37.046	Stop	Typical Windows Stop Time	637856820	$LogFile
Forged (Foreign Computer Attachment)	Document Creation	Critical Documents Used By Prosecution	637868334-638077281	$LogFile
N/A (Foreign Computer Attachment)	Document Deletion	Critical Documents Used By Prosecution	638081144-638157265	$LogFile
02/11/2011 20:54:11.609	Start	Suspicious Windows Start Time	638168609	$LogFile
02/11/2011 20:55:16.328	Stop	Suspicious Windows Stop Time	638169993	$LogFile
2/14/2011 04:00:00 (Approximately)	Police Raid Odatv	Turkish National Police Raid Odatv	N/A	External

Table 12. Partition 2 – Suspicious Activity Summary
* Windows Start/Stop = Last Accessed (Standard Information Attribute)

Light Blue = Windows Start
Dark Blue = Windows Stop
Grey = Suspicious Event

Ahtapot development seems to have been quite professional. Even the symbol paths hint at organized development:

E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Tohum_h.pdb

E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Beyin_h.pdb

E:\Projeler\Ahtapot\Release\Ahtapot_h[Beta]\Release\Kol_8_h.pdb

What the attackers apparently failed to realize prior to leaving Odatv the evening of February 11 was that Ahtapot was unable to install itself properly. After briefly booting Mr. Pehlivan's Odatv computer

Ahtapot Component	Filename	MD5 Hash Value
Tohum (Seed)	windows.exe	003c95d26571003oca4c18baf9ba6a61
Beyin (Brain)	svchost.exe	58d6e15ce9d3081b5ef5eb1b70d7cbbo
Kol (Arm)	trp.exe	961cef5861317dd9966dc3f6eb5387d8

Table 10. Ahtapot Components

Event	Event Detail	Command & Control	Date/Time (UTC)*
Local RAT Attack (Thumb Drive Attachment)	Turkojan	haber.sytes.net	01/14/2011 13:56:05
Email RAT Attack	Turkojan	blogg.serveblog.net	01/21/2011 14:13:14
Local RAT Attack (Thumb Drive Attachment)	Turkojan	N/A (Not Dropped) **	01/25/2011 18:57:15
Email RAT Attack	Turkojan with Decoy	tigereyes2.servepics.com	01/27/2011 05:57:44
Email RAT Attack	Turkojan with Decoy	driver.myftp.org	01/31/2011 04:33:20
Email RAT Attack	Turkojan	antivirus.myftp.org	02/03/2011 11:07:09 – 02/03/2011 10:58:39
Email RAT Attack	Turkojan	antivirus.myftp.org	02/05/2011 01:31:42 – 02/05/2011 01:31:44
Email RAT Attack	Bandook with Exploit & Decoy	adobupdate.serveftp.com	02/05/2011 20:49:56 – 02/05/2011 20:58:04
Email RAT Attack	Bandook with Decoy	adobupdate.serveftp.com	02/05/2011 21:33:54.000
Local RAT Attack (Hard Drive Removal)	Bandook	adobupdate.serveftp.com	02/09/2011 (Evening)
Local RAT Attack (Hard Drive Removal)	Ahtapot	adobupdate.serveftp.com	02/11/2011 (Evening)
Police Raid Odatv	Turkish National Police Raid Odatv	N/A	2/14/2011 04:00:00 (Approximately)

Table 13. RAT Attack Summary
*Local RAT Attacks = Relative Time, Email RAT attacks = Email Time
** Not dropped due to a similar self-inflicted wound which prevented Ahtapot from being fully dropped

just prior to 11pm, Ahtapot was only partially installed because the "seed" could not create the "brain." Did Odatv have some kind of sophisticated technology that prevented the creation of Ahtapot's brain on Mr. Pehlivan's Odatv computer? The simple answer is no; the attackers were foiled by one of their previous RATs having created a component with the same filename, in the same location, as that which Ahtapot attempted to create. In other words, the attackers "last resort" RAT attack was thwarted by a previous attack.

/ SUSPICIOUS ACTIVITY SUMMARY

Let's summarize in Tables 11 and 12 what we have learned about the local attacks on February 9 and 11, along with "external anchors" (dates and times existing outside the electronic evidence in question, which could be gathered from court orders, video footage, news articles, etc.).

/ EARLIER ATTACKS

The local attacks against Mr. Pehlivan's Odatv computer, revealed by the application of ART, did not exist in a vacuum. The local attacks on February 9 and 11 occurred only after a series of earlier local and remote (via email) attacks. We have reason to believe these attacks were unsuccessful. Unsuccessful, but not amateur.

Consider, just cursorily for now in Table 13, the RAT attacks against Mr. Pehlivan's Odatv computer that Arsenal identified from January 2011 onward.

One can now understand, given previous failures involving both local and remote attacks, why the attackers locally copied incriminating documents to Mr. Pehlivan's Odatv computer hard drive on the evenings of February 9 and 11 along with RATs which, if working as intended, would have allowed the incriminating documents to be placed remotely. Was this methodology successful? You decide, all the RAT attacks mentioned in Table 13 appear to have failed, but the prosecution was able to proceed with the documents created locally on Mr. Pehlivan's Odatv computer hard drive.

The analysis as described here only scratches the surface of what Arsenal has found within electronic evidence on which the Ergenekon and Sledgehammer trials were based. There are more victims, more computers, and more attacks worthy of discussion. For now, remember that leveraging ART may be the only way out of the fog when attackers have gone to great lengths to deceive you.

/ TOOLS

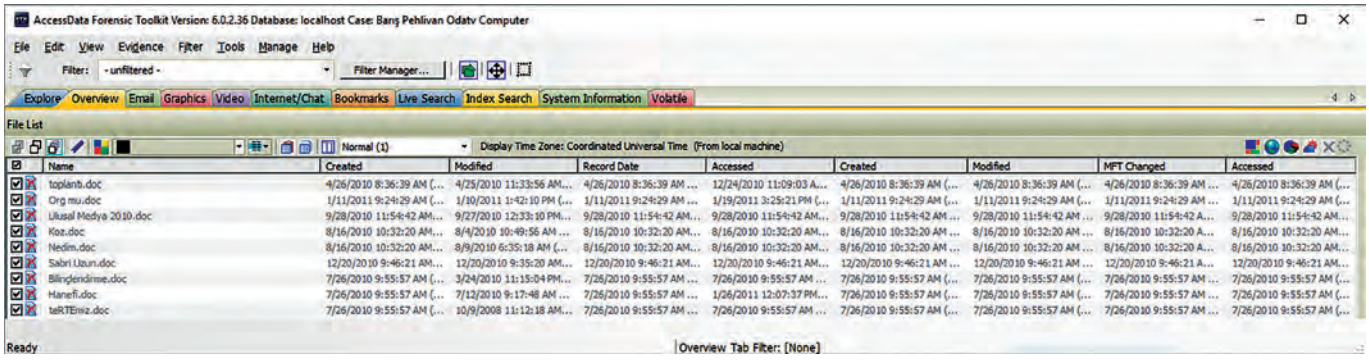
Examples of tools used during the analysis described in this article:

- Event Log Explorer (FSPro Labs) – eventlogxp.com
- LogFileParser (Joakim Schicht) – github.com/jschicht/LogFileParser
- Mft2Csv (Joakim Schicht) – github.com/jschicht/Mft2Csv
- Registry Recon (Arsenal Recon) – ArsenalRecon.com/apps/recon/
- ssdeep (Jesse Kornblum) – ssdeep.sourceforge.net/
- UsnJrnl2Csv (Joakim Schicht) – github.com/jschicht/UsnJrnl2Csv

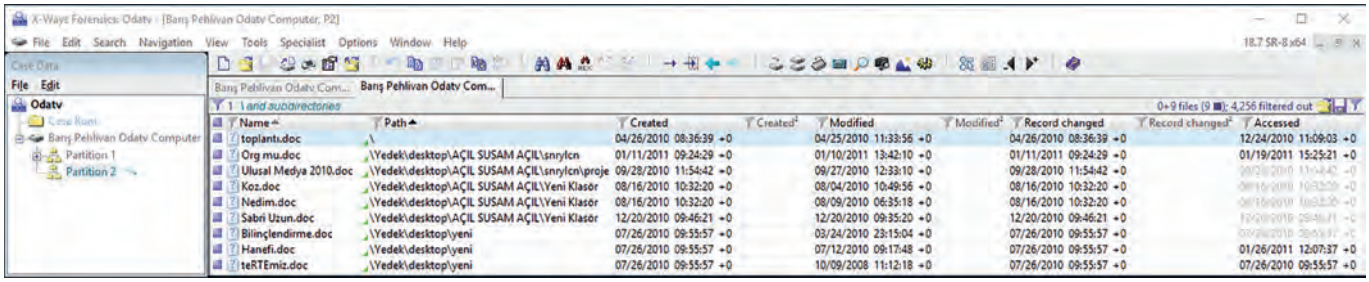
/ DEFINITIONS

NTFS is a journaling file system developed by Microsoft as a more functional and reliable successor to their FAT file systems. NTFS was first released with Windows NT 3.1 and remains the default file system in Windows 10.

The $LogFile (NTFS Log) metafile is a file system transaction log on each NTFS volume that provides redo and undo functionality by using unique identifiers for transactions called LSNs (Log Sequence Numbers). In other words, the $LogFile keeps track of file system transactions so they can be redone, or undone, if



Critical documents created & deleted February 11, 2011 as seen by AccessData's FTK



Critical documents created & deleted February 11, 2011 as seen by X-Ways Software Technology AG's X-Ways Forensics

necessary. The $LogFile is a critical part of NTFS's journaling functionality which reduces the likelihood of corruption to the file system's core in the event of system crashes. LSNs normally increase sequentially (occurring in the order in which changes to files, folders, and their metadata happen) regardless of their associated dates and times.

The $MFT (Master File Table) metafile on each NTFS volume keeps track of files and folders by maintaining information about their names, locations, dates and times, and 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 normally increase sequentially in the order in which files and folders were created, regardless of their associated dates and times.

The $Secure metafile on each NTFS volume contains security descriptors used to control access to files and folders. Access control information found in security descriptors identifies who can access objects and how. Each security descriptor is associated with a SecurityId for more efficient reference by other NTFS metafiles which include the $MFT, $LogFile, and $UsnJrnl. SecurityIds normally increase sequentially in the order in which they were added to the $Secure metafile, regardless of the dates and times associated with the operating system responsible for adding them.

The $UsnJrnl (Update Sequence Number Journal or Change Journal) metafile is an optional file system transaction log on each NTFS volume made available to third-party applications (e.g., malware scanning and backup applications). The $UsnJrnl on each volume essentially stores a subset of information stored by the $LogFile in a more human-friendly way. $UsnJrnl records are identified using USNs (Update Sequence Numbers). USNs normally increase sequentially (occurring in the order in which changes to files, folders, and their metadata happen) regardless of their associated dates and times.

Event Logs are diagnostic files maintained by Windows and certain applications. Depending on how Windows is configured, it may be possible to determine when the system started and stopped, when users logged in and out, when software applications were installed and removed, and much more. Each event in an event log is assigned a RecordNumber or EventRecordID (depending on the version of Windows – "Event Logging" or "Windows Event Log"), which normally increases sequentially, regardless of the dates and times associated with that event. /

/ AUTHOR BIOGRAPHY

Mark Spencer is President of Arsenal Consulting, where he leads engagements involving digital forensics for law firms, corporations, and government agencies. Mark is also President of Arsenal Recon, where he guides development of digital forensics tools. Mark has more than 15 years of law-enforcement and private-sector digital forensics experience. He 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 is headquartered in the Chelsea Naval Magazine, a historic military structure in which arms for the celebrated heavy frigate USS Constitution were stored, 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