

Unraveling the Digital Footprints of Willy B. Yeat's Desktop

As part of my latest digital forensics investigation, I delved into the mysteries hidden within Willy B. Yeat's desktop system. My goal was to piece together a timeline of digital activity, uncover user behavior, and identify connected devices that could provide critical clues. Below, I'll share my findings and highlight the discrepancies and insights I uncovered during the investigation. Screenshots and source data referenced throughout can be found in the appended "Figures" section.

Starting with the Basics: Building a Timeline

I began by trying to establish a timeline of activity on the device. The system revealed multiple user accounts, including *john.mccrae*, *Ted.Rethke*, *WillyB*, and *yeatsw*. To pinpoint the last active user, I examined the software registry hive, which showed *yeatsw* as the most recent login (Figure 1).

Next, I explored the NTUSER.DAT file associated with *yeatsw*. Using the forensics tool "Autopsy," I identified metadata indicating the last modification to this file—March 7, 2021, at 17:22 (Figure 2).

To corroborate this, I checked the most recent shutdown time in the system registry hive. This data, stored as a hexadecimal value (Figure 3), converted to December 13, 2020, at 14:07. Here's where things got interesting: there's a clear discrepancy between the last recorded user activity and the last shutdown. This suggests the device either ran continuously for three months, experienced a system crash, or had its clock manipulated. Files accessed during this period are likely worth a closer look.

Digging into Connected Devices

The next step was to examine devices connected to the system. The system registry hive provided information on two storage devices:

1. An unbranded USB flash drive last connected on March 8, 2021.
2. A SanDisk SD card last connected on December 8, 2020 (Figure 4).

Diving deeper, I analyzed USB activity logs. On the morning of March 8, 2021, there was a flurry of activity (Figure 5). It included the unbranded flash drive, USB human interface devices (keyboards or mice), USB hubs, and a composite device. Notably, an Intel Bluetooth adapter was also detected.

This activity raised another discrepancy: it occurred approximately eight hours after *yeatsw*'s last recorded activity. Since no user login was recorded during this time, the activity could have been at the system level or triggered by automated tasks.

Tracing Online Activity and Software Usage

Focusing back on *yeatsw*, I investigated recently typed URLs in Internet Explorer. Unfortunately, this led to a dead end—a Bing homepage URL (Figure 6).

Next, I reviewed installed executables, which were mostly standard Windows programs, except for one outlier: *Thunderbird.exe* (Figure 7). Thunderbird, an open-source email client, was last executed on March 7, 2021, at 17:07—just 15 minutes before *yeatsw*'s final recorded activity.

Exploring *yeatsw*'s application data revealed stored emails, including one confession (Figure 9) detailing the use of SQL injection to steal two birth records. This email also referenced a trip to Vancouver around November 23, 2020.

Uncovering the Smoking Gun

The most damning evidence came from further examination of *Thunderbird*. In Figure 10, I found a photograph of what appear to be stolen passports, plane tickets, and two individuals. The boarding passes indicate travel from San Francisco to Mexico City and onward to Port Vila, scheduled for March 12–13, 2021.

Adding to the intrigue, Figure 11 contained coordinates pointing to an island off the coast of Vanuatu.

Key Discrepancies and Next Steps

Several discrepancies stood out during this investigation:

- The USB flash drive activity eight hours after *yeatsw*'s last login raises questions about system-level or automated actions.
- The Thunderbird email client played a central role in revealing critical evidence, suggesting it warrants further examination.

This initial analysis has provided valuable leads, from a potential hiding place to a suspicious timeline of events. The investigation is far from over, but these findings bring us one step closer to unraveling Willy B. Yeat's activities.

Figures

Figure 1

LastLoggedOnUser	RegSz	BYZANTIUMUS\yeatsw	74-00-68-00-6B-00-65-00-00...
------------------	-------	--------------------	-------------------------------

*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOn
User*

Figure 2

Metadata	
Name:	/img_W2025.001/vol_vol3/Users/yeatsw/NTUSER.DAT
Type:	File System
MIME Type:	application/x.windows-registry
Size:	1048576
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2021-03-07 17:22:14 PST

Autopsy metadata for yeatsw's NTUSER.DAT file

Figure 3

ShutdownTime	RegBinary	E4-A1-D4-48-59-D1-D6-01	23-4A-53-05
--------------	-----------	-------------------------	-------------

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Windows\ShutdownTime

```
import datetime

hex_value = "01D6D15948D4A1E4"

timestamp = int(hex_value, 16)

shutdown_time = datetime.datetime(1601, 1, 1) + datetime.timedelta(microseconds=timestamp // 10)

print("Shutdown Time (UTC):", shutdown_time)
```

2020-12-13 14:07:25.819748

Figure 4

2020-11-23 22:24:19	Ven_Generic	Prod_Flash_Disk	Rev_8.07	38A261A4&0	Generic Flash Disk USB Device	{99e950a6-283d-11e1-b-e9fd-8cd0c44e75df }	2020-11-23 22:24:19	2020-11-23 22:24:19	2021-03-08 01:06:10
2020-11-19 07:50:58	Ven_SanDisk	Prod_Ultra	Rev_1.00	-4C531001330607117133&0	SanDisk Ultra USB Device	{f49ac797-2a3b-11e1-b-e9fd-8cd0c44e75df }	2020-11-19 07:50:58	2020-11-19 07:50:58	2020-12-08 06:36:12




HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

Figure 5

2021-03-08 01:06:10	VID_058F&PID_6387	38A261A4			USBSTOR	USB Mass Storage Device		Port_#0006.Hub_#0003
2021-03-08 01:22:37	VID_046D&PID_C066	7F8E8A43900018	68748fef00		usbccgp	USB Composite Device		Port_#0006.Hub_#0002
2021-03-08 01:22:37	VID_046D&PID_C066&MI_00	68748fef00&0000	7874cfd0f0		HidUsb	USB Input Device		0000.0014.0000.006.000.000.000.000.000
2021-03-08 01:22:37	VID_046D&PID_C066&MI_01	68748fef00&0001	782fb7aba0		HidUsb	USB Input Device		0000.0014.0000.006.000.000.000.000.000
2021-03-08 01:22:55	ROOT_HUB30	48206037800&0	58376aba20		USB4UB3	USB Root Hub (USB 3.0)		
2021-03-08 01:22:55	ROOT_HUB30	781c55d63b00&0			USB4UB3	USB Root Hub (USB 3.0)		
2021-03-08 01:22:55	VID_045E&PID_0000	58376aba20&0&5	681fb772ea0		usbccgp	USB Composite Device		Port_#0005.Hub_#0002
2021-03-08 01:22:55	VID_045E&PID_0000&MI_00	681fb772ea0&0000	782a10aa0e0		HidUsb	USB Input Device		0000.0014.0000.005.000.000.000.000.000
2021-03-08 01:22:55	VID_045E&PID_0000&MI_01	681fb772ea0&0001	786396ccc0		HidUsb	USB Input Device		0000.0014.0000.005.000.000.000.000.000
2021-03-08 01:22:56	VID_8087&PID_0A2B	58376aba20&0&13						Port_#0013.Hub_#0002

HKLM\SYSTEM\CurrentControlSet\Enum\USB

Figure 6

Timestamp	Url	Slack
==		
	http://go.microsoft.com/fwlink/?LinkId=255141	U 

HKEY_USERS\SOFTWARE\Microsoft\Internet Explorer\TypedURLs

Figure 7

2020-11-08 00:36:44	thunderbird.exe	C:\Program Files\Mozilla Thunderbird\thunderbird.exe	C:\Program Files\Mozilla Thunderbird
---------------------	-----------------	--	--------------------------------------

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths

Figure 8

thunderbird.exe	▼	2021-02-
thunderbird.VisualElementsManifest.xml		2021-02-
ucrtbase.dll		2021-02-
update-settings.ini		2021-02-
updater.exe	▼	2021-02-
updater.ini		2021-02-
vcruntime140.dll		2021-02-
WSEnable.exe	▼	2021-02-
xul.dll	▼	2021-02-

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis
Go to Result						
Program Execution: Program Run On 2020-12-07 22:44:00 PST						
Go to Result						
Program Execution: Program Run On 2020-12-07 22:44:00 PST						
Go to Result						
Program Execution: Program Run On 2020-12-07 22:45:00 PST						
Go to Result						
Program Execution: Program Run On 2021-03-07 17:07:54 PST						
Go to Result						

Autopsy Context for thunderbird.exe

Figure 9

Found that someone isn't very careful with their coding. A little SQL injection and, viola, 2 birth records added. From there it was just a matter of ordering a copy of our birth certificates.

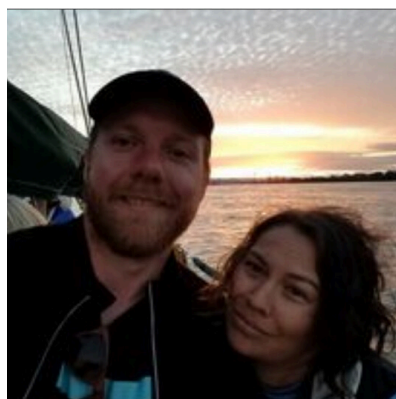
Once I was up there, it was easy to get the passports. The nice lady made an exception for you being present, given that we'd been away on a mission with our parents for the last several years and you wanted to get home so bad for our wedding. :)

Still open for a trip to Vancouver on Saturday?

On 11/23/2020 2:58 PM, Maud Gonne wrote:

Users\yeatsw\AppData\Roaming\Profiles\bo0pat20.default-release\mail\byzantiumus.com found using the Autopsy

Figure 10



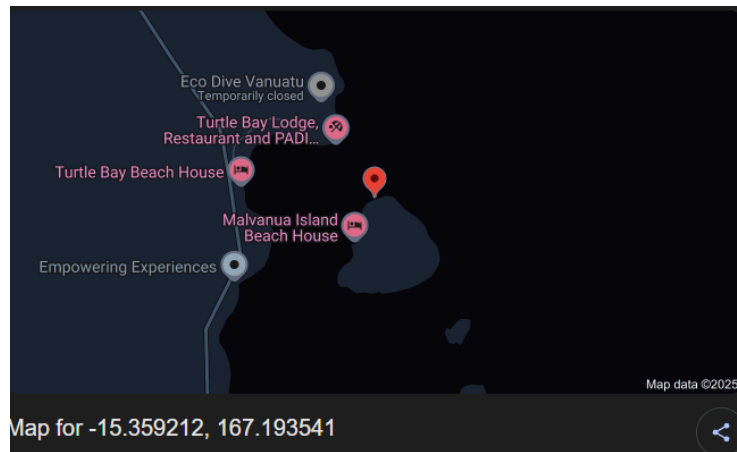
Users/yeatsw/AppData/Roaming/Profiles/bo0pat20.default-release/mail/byzantiumus.com/sent
found using the Autopsy

Figure 11

Money has been moved. You know the plan. Text me as soon as you get this, so I can delete the server and throw this system away--I have to move fast if I'm going to make my flight after driving from Astoria.

If for some reason we can't connect in Mexico City, keep going--I'll meet you there. Malvanua. -15.359212, 167.193547. We own the whole thing, so stay in the big house. :)

Print these out, then throw your laptop in the river.



Users/yeatsw/AppData/Roaming/Profiles/bo0pat20.default-release/mail/byzantiumus.com found using the Autopsy