Gwynedd Mercy University

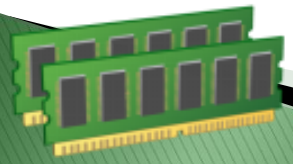
RAM Analysis

Memory Forensics

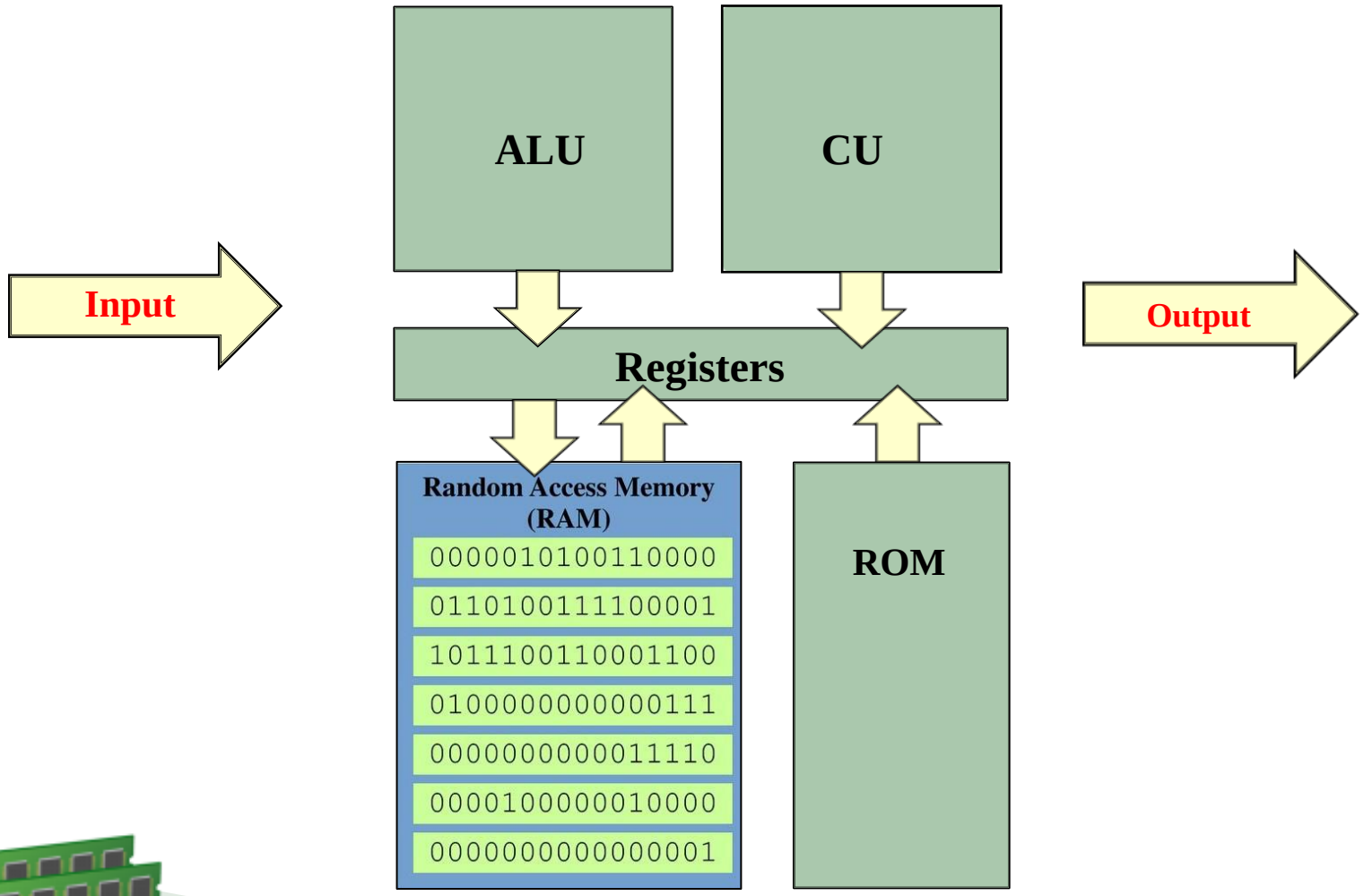
Cindy Casey
casey.cindy@gmercyu.edu

What is RAM?

- **Random Access Memory**
  - Hardware (integrated circuit) that allows data to be stored and retrieved on a computer.
  - Data accessed randomly instead of sequentially like it is on a CD or hard drive.
  - Computer can access data in RAM much faster than ROM.
- **RAM is volatile**
  - Volatile memory requires power to keep the data accessible

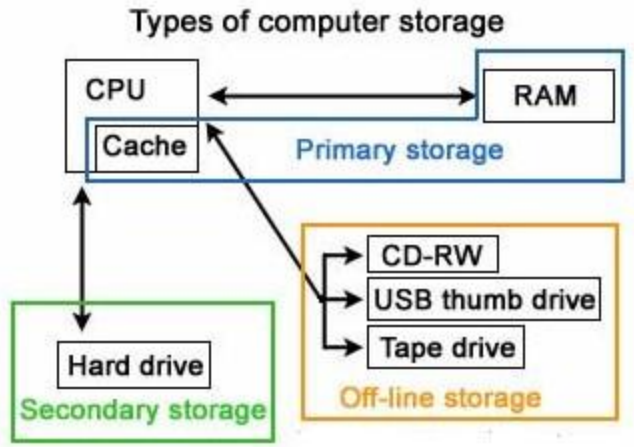


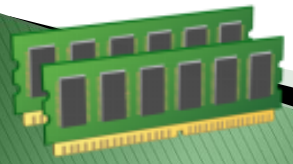
Von Neumann Architecture



Memory

- While both the HD and RAM are memory, RAM is referred to as primary memory (or just memory) and the hard drive as storage or secondary storage.





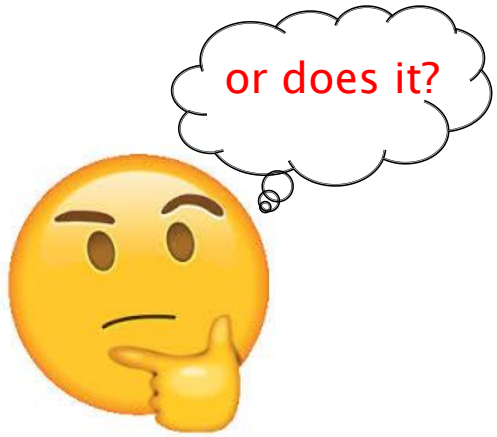
Where can we find RAM?

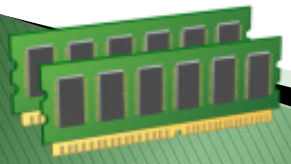
Dead-Box verses Live-Box Analysis

Traditional computer forensics focuses on Dead-Box analysis.

- Accessing and analyzing Non-volatile information.
- Non-volatile data is maintained when the device is powered off.
- Also known as persistent storage.

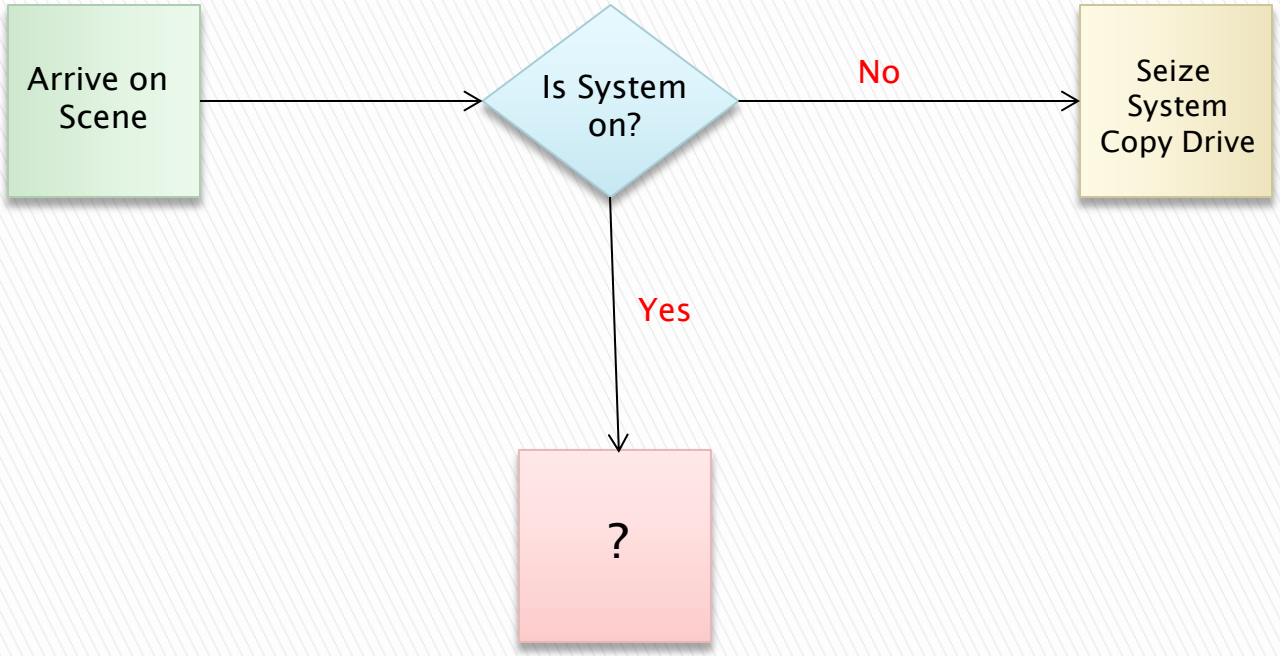
- **Emerging need to focus on Live-Box analysis**
  - Accessing and analyzing Volatile information.
  - Volatile data is only maintained while the device is powered on.
  - Once the device is powered down the data flushes away…





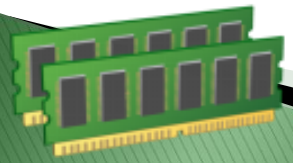
Dead-Box verses Live-Box Analysis

- **Currently only two states a system can be in during an incident response or when seizing evidence:**
  1. Dead System – Turned off
  2. Live System – Running



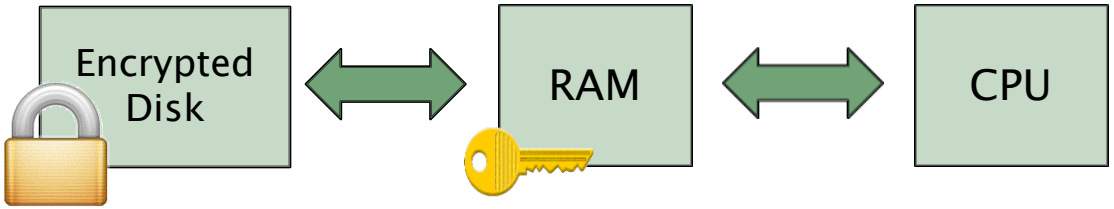
Artifacts that Might be Found in RAM

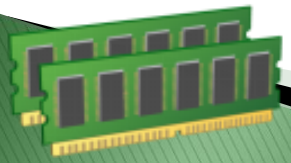
- Past and current network connections
- Running processes at the time of RAM capture
- User names and **passwords**
- Loaded Dynamically Linked Libraries (DLL)
- Contents of an open window
- System information (i.e.: time since last reboot)
- Recreate the Task Manger
- Data never written to the hard disk drive
- Rootkits
- Registry Information
- Memory resident malware (fileless malware)
- **Encryption keys**



Extracting Encryption Keys from RAM

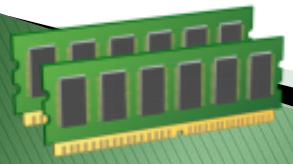
- Before they can be run by the processor, programs (including data and instructions) must be loaded into physical or main memory.
- This includes any software that encrypts (key must be loaded into memory).
- The key resides in the RAM until the machine is powdered off.
- Dumping the contents of the RAM while the machine is running increases the likelihood of retrieving the key.





Memory Resident Malware

- Malware which may never even touch the hard drive.
- Can exist completely in RAM.
- Becoming more resistant.
- Leaves no footprint on hard drive.
- Can’t be detected using traditional forensic methodologies.
- Not detected by anti-virus software or auditing techniques.
- Part of many sophisticated attacks today.



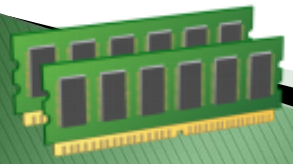
Fileless Malware on the Rise

by Tomas Meskauskas on October 2, 2019

According to reports analyzing the state of the threat landscape, fileless malware incidents are up to some 265% in the first half of 2019 when compared to the same period in 2018. Fileless malware sometimes has been referred to as a zero-footprint attack or non-malware attack. However, fileless malware may be the best name for the attack method, as the attack is not

LATENTBOT

- Multiple layers of obfuscation.
- Payload never touches the victims' hard drive.
- Custom encryption algorithm.
- Capable of watching victims without ever being noticed.
- Can corrupt a HD – rendering PC useless.
- Ransomlock similarities (i.e.: can lock the desktop).
- Stealthy - only keeps malicious code in memory for time it is needed.



LatentBot malware opens a backdoor on the finance industry

David Bisson | December 14, 2015 9:24 pm | Filed under: **Botnet**, **Malware**, **Phishing**, **Privacy**, **Vulnerability**, **Windows**

Security researchers have uncovered the LatentBot malware, a sophisticated and unusual attack that is using multiple levels of obfuscation to target companies in the financial and insurance industries around the world.

In a **report** published on FireEye's blog, analysts Taha Karim and Daniel Regalado explain that the malware has been involved in multiple campaigns against enterprises located in the United States, the UK, Brazil, South Korea, Canada, and elsewhere.

> "Although the infection strategy is not new, the final payload dropped – which we named LatentBot – caught our attention since it implements several layers of obfuscation, a unique exfiltration mechanism, and has been very successful at infecting multiple organizations."

LatentBot is dropped as the third-stage binary in an infection process that begins with a Microsoft Word exploit. Attackers create the malicious Word document using Microsoft Word Intruder (MWI); once the document is opened, a malicious executable runs and downloads the LuminosityLink Remote Access Trojan (RAT) as the second-stage binary.

Enron: What Caused the Ethical Collapse?

Introduction

Kenneth Lay, former chairman and chief executive officer (CEO) of Enron Corp., is quoted in Michael Novak's book *Business as a Calling: Work and the Examined Life* as saying, "I was fully exposed to not only legal behavior but moral and ethical behavior and what that means from the standpoint of leading organizations and people." In an introductory statement to the revised *Enron Code of Ethics* issued in July 2000, Lay wrote: "As officers and employees of Enron Corp., its subsidiaries, and its affiliated companies, we are responsible for conducting the business affairs of the companies in accordance with all applicable laws and in a moral and honest manner." Lay went on to indicate that the 64-page *Enron Code of Ethics* reflected policies approved by the company's board of directors and that the company, which enjoyed a reputation for being fair and honest, was highly respected. Enron's ethics code also specified that "An employee shall not conduct himself or herself in a manner which directly or indirectly would be detrimental to the best interests of the Company or in a manner which would bring to the employee financial gain separately derived as a direct consequence of his or her employment with the Company."

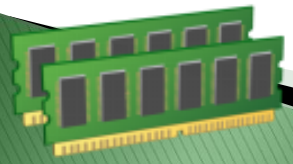
Enron's ethics code was based on respect, integrity, communication, and excellence. These values were described as follows:

> Respect. We treat others as we would like to be treated ourselves. We do not tolerate abusive or disrespectful treatment. Ruthlessness, callousness and arrogance don't belong here.
> Integrity. We work with customers and prospects openly, honestly and sincerely. When we say we will do something, we will do it; when we say we cannot or will not do something, then we won't do it.
> Communication. We have an obligation to communicate. Here we take the time to talk with one another . . . and to listen. We believe that information is meant to move and that information moves people.
> Excellence. We are satisfied with nothing less than the very best in everything we do. We will continue to raise the bar for everyone. The great fun here will be for all of us to discover just how good we can really be.

Given this code of conduct and Ken Lay's professed commitment to business

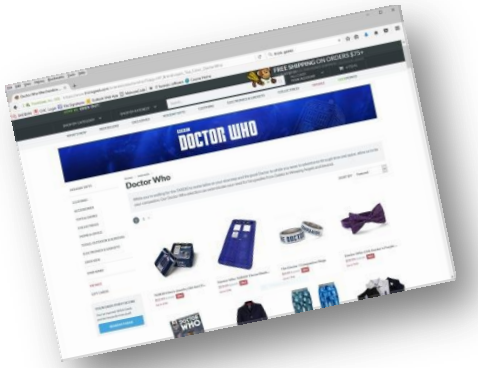
RAM Scraping Attacks on the Rise

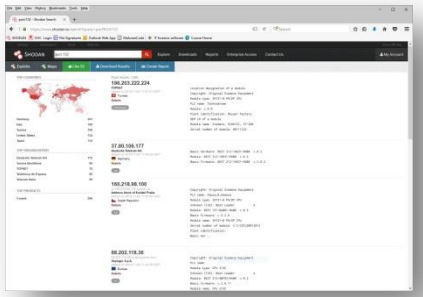
- **Point of Sale (POS) RAM Scraper Malware Attacks are on the rise**
  - Steals payment data from RAM of POS systems.
  - Payment Card Industry Data Security Standard (PCI-DSS) requires end-to-end encryption.
  - Payment data is decrypted in POS's RAM for processing.
  - This is where RAM Scraper comes in.
  - Searches to harvest clear-text payment data.
  - Data then sent to rogue call-home server.
- **Even smart cards are not safe from these types of attack!**

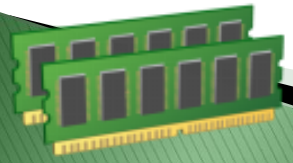


RAM Scraping…
Not just for Server-Side Attacks

- Client-side attacks are also probable.
- Browsers are famous for leaving artifacts in memory during web sessions.
- RAM scraping malware can target encryption keys in memory to decrypt anything from session data to encrypted files.

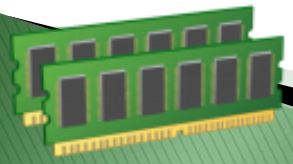


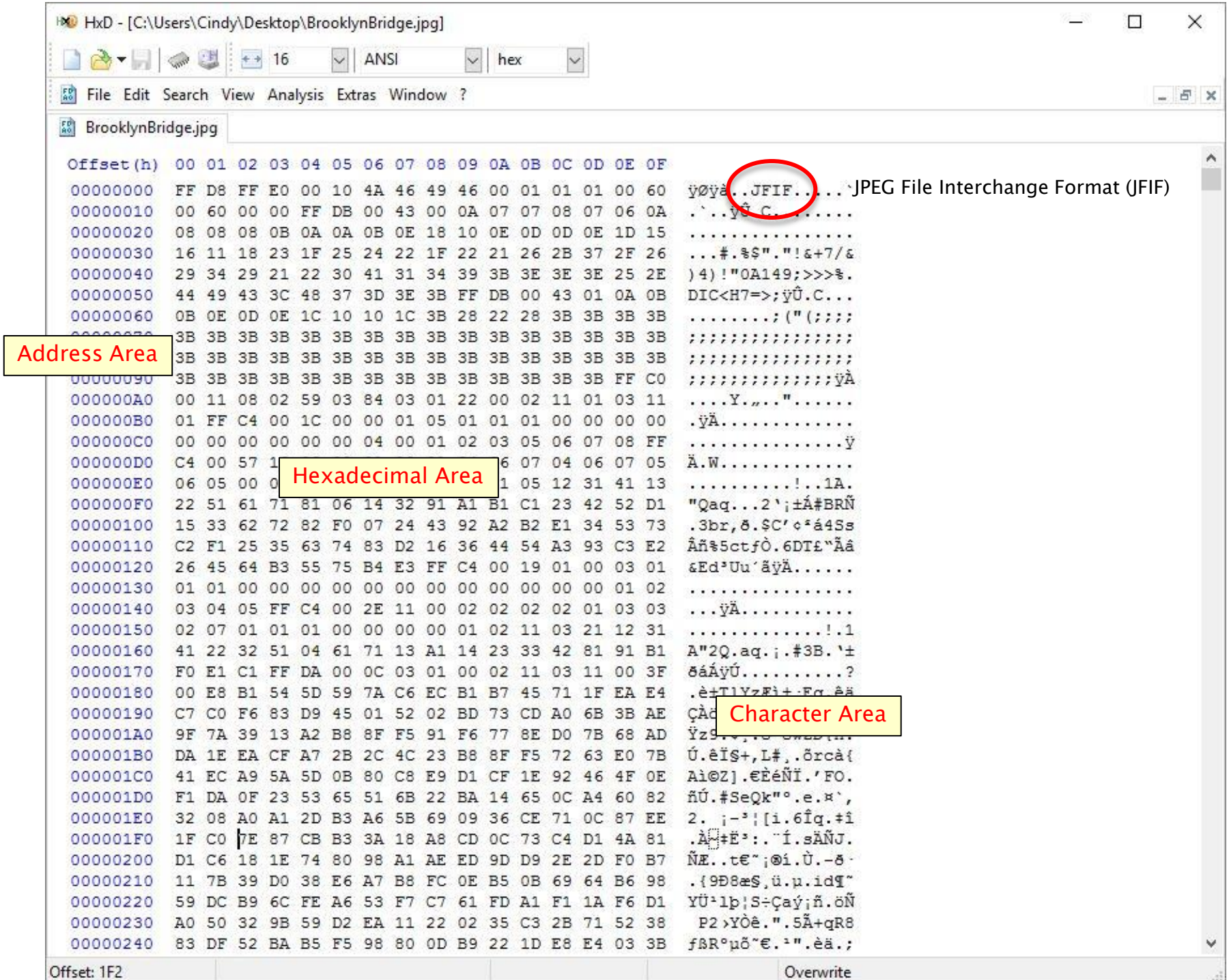




Memory Acquisition

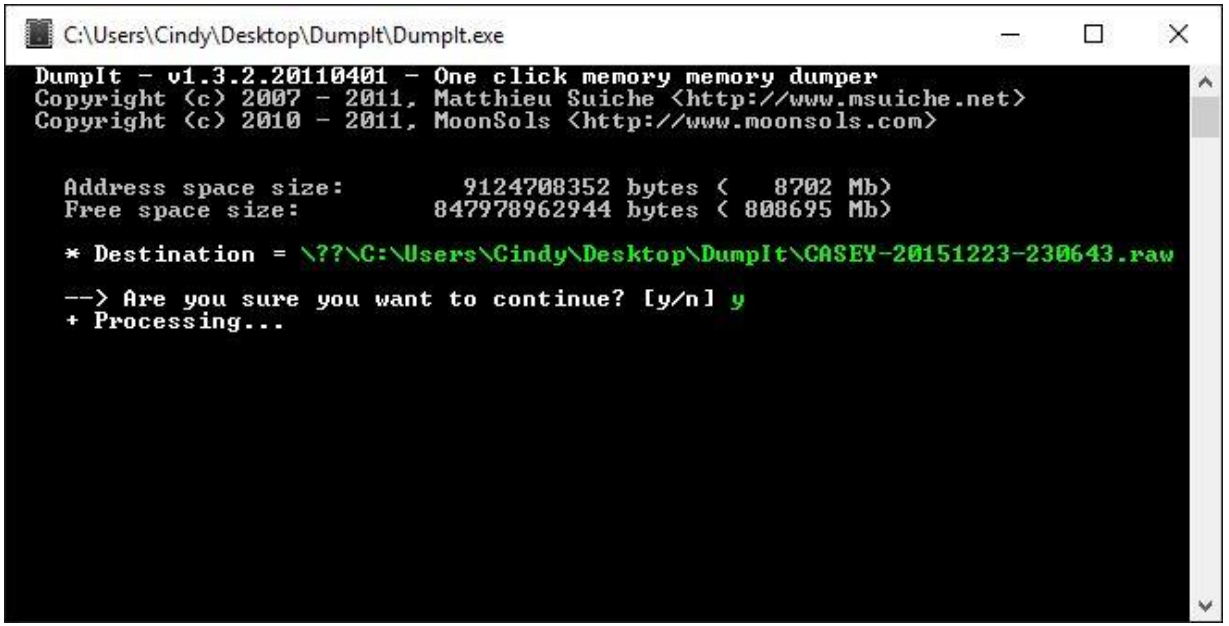
- It is crucial to acquire volatile evidence before any other type of acquisition.
- Live forensic tools make substantial changes to volatile memory.
- **We will look at several tools**
  - Hex Editor
  - DumpIt RAM Capture Utility
  - Belkasoft RAM Capturer - Volatile Memory Acquisition Tool
  - FTK

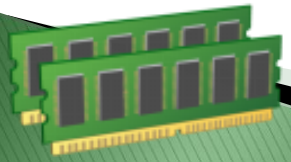



HxD - [C:\Users\Cindy\Desktop\BrooklynBridge.jpg]
16
ANSI
hex
File Edit Search View Analysis Extras Window ?
BrooklynBridge.jpg
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 ÿØÿà..JFIF.....`
00000010 00 60 00 00 FF DB 00 43 00 0A 07 07 08 07 06 0A .`..ÿÛ.C.....
00000020 08 08 08 0B 0A 0A 0B 0E 18 10 0E 0D 0D 0E 1D 15 ....
00000030 16 11 18 23 1F 25 24 22 1F 22 21 26 2B 37 2F 26 ...#.%$".!&+7/&
00000040 29 34 29 21 22 30 41 31 34 39 3B 3E 3E 3E 25 2E)4)!"0A149;>>>%.
00000050 44 49 43 3C 48 37 3D 3E 3B FF DB 00 43 01 0A 0B DIC<H7=>;ÿÛ.C...
00000060 0B 0E 0D 0E 1C 10 10 1C 3B 28 22 28 3B 3B 3B 3B ....;("(;;;;
000000A0 00 11 08 02 59 03 84 03 01 22 00 02 11 01 03 11 ....Y.„.."......
000000B0 01 FF C4 00 1C 00 00 01 05 01 01 01 00 00 00 00 .ÿÄ.............
000000C0 00 00 00 00 00 00 04 00 01 02 03 05 06 07 08 FF ....ÿ
000000D0 C4 00 57 1 6 07 04 06 07 05 Ä.W.............
000000E0 06 05 00 0 1 05 12 31 41 13 ....!..1A.
000000F0 22 51 61 71 81 06 14 32 91 A1 B1 C1 23 42 52 D1 "Qaq...2'¡±Á#BRÑ
00000100 15 33 62 72 82 F0 07 24 43 92 A2 B2 E1 34 53 73 .3br‚ð.$C'¢²á4Ss
00000110 C2 F1 25 35 63 74 83 D2 16 36 44 54 A3 93 C3 E2 Âñ%5ctƒÒ.6DT£"Ãâ
00000120 26 45 64 B3 55 75 B4 E3 FF C4 00 19 01 00 03 01 &Ed³Uu´ãÿÄ......
00000130 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 ....
00000140 03 04 05 FF C4 00 2E 11 00 02 02 02 02 01 03 03 ...ÿÄ...........
00000150 02 07 01 01 01 00 00 00 00 01 02 11 03 21 12 31 ....!.1
00000160 41 22 32 51 04 61 71 13 A1 14 23 33 42 81 91 B1 A"2Q.aq.¡.#3B.'±
00000170 F0 E1 C1 FF DA 00 0C 03 01 00 02 11 03 11 00 3F ðáÁÿÚ..........?
00000180 00 E8 B1 54 5D 59 7A C6 EC B1 B7 45 71 1F EA E4 .è±T]YzÆì±·Eq.êä
00000190 C7 C0 F6 83 D9 45 01 52 02 BD 73 CD A0 6B 3B AE ÇÀö.ÙE.R.½sÍ k;®
000001A0 9F 7A 39 13 A2 B8 8F F5 91 F6 77 8E D0 7B 68 AD Ÿz9.¢¸.õ'öwŽÐ{h.
000001B0 DA 1E EA CF A7 2B 2C 4C 23 B8 8F F5 72 63 E0 7B Ú.êÏ§+,L#¸.õrcà{
000001C0 41 EC A9 5A 5D 0B 80 C8 E9 D1 CF 1E 92 46 4F 0E Aì©Z].€ÈéÑÏ.'FO.
000001D0 F1 DA 0F 23 53 65 51 6B 22 BA 14 65 0C A4 60 82 ñÚ.#SeQk"º.e.¤`‚
000001E0 32 08 A0 A1 2D B3 A6 5B 69 09 36 CE 71 0C 87 EE 2. ¡-³¦[i.6Îq.‡î
000001F0 1F C0 7E 87 CB B3 3A 18 A8 CD 0C 73 C4 D1 4A 81 .À~‡Ë³:.¨Í.sÄÑJ.
00000200 D1 C6 18 1E 74 80 98 A1 AE ED 9D D9 2E 2D F0 B7 ÑÆ..t€˜¡®í.Ù.-ð·
00000210 11 7B 39 D0 38 E6 A7 B8 FC 0E B5 0B 69 64 B6 98 .{9Ð8æ§¸ü.µ.id¶˜
00000220 59 DC B9 6C FE A6 53 F7 C7 61 FD A1 F1 1A F6 D1 YÜ¹lþ¦S÷Çaý¡ñ.öÑ
00000230 A0 50 32 9B 59 D2 EA 11 22 02 35 C3 2B 71 52 38 P2›YÒê."..5Ã+qR8
00000240 83 DF 52 BA B5 F5 98 80 0D B9 22 1D E8 E4 03 3B ƒßR°µõ˜€.¹".èä.;
Address Area
Hexadecimal Area
Character Area
JPEG File Interchange Format (JFIF)
Offset: 1F2
Overwrite

Dumpit.exe

- Open Source Tool.
- Raw memory dump generated and saved to same directory as DumpIt.exe (.mem file).



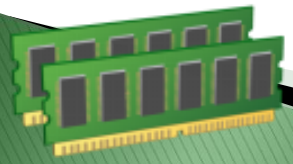


1. Open tool
2. Select yes (y)
3. When completed you will see the word success

Now Comae Technologies

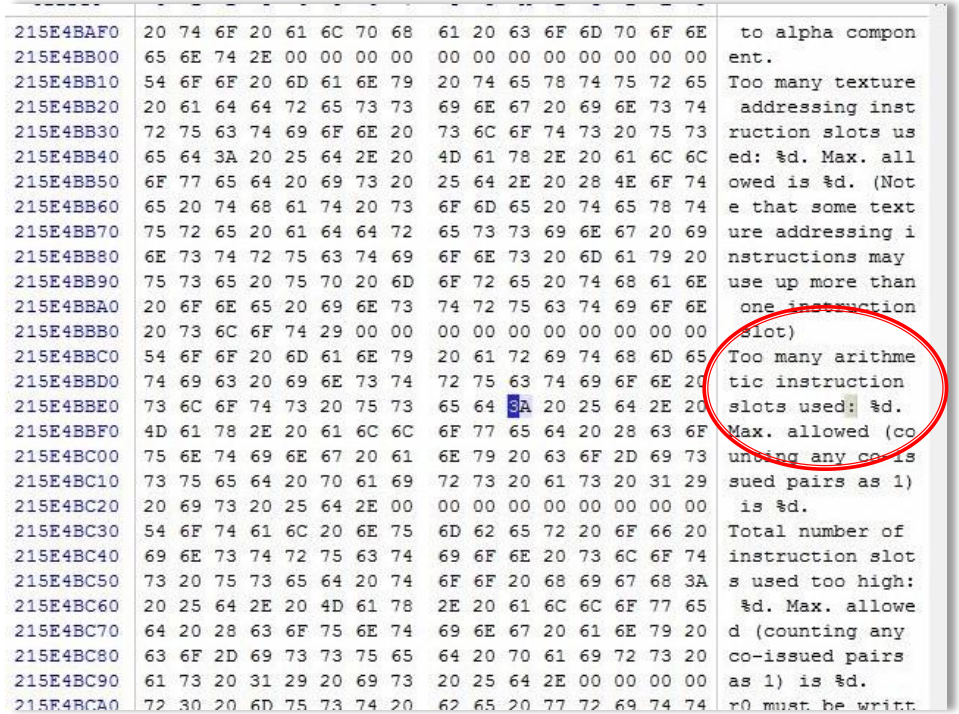
C:\Users\Cindy\Documents\Comae-Toolkit-3.0.20190919.1\x64\DumpIt.exe

```
DumpIt 3.0.20190919.1 (X64) (Sep 19 2019)
Copyright (C) 2007 - 2020, Matt Suiche (msuiche)
Copyright (C) 2016 - 2020, Comae Technologies DMCC <https://www.comae.com>
All rights reserved.

DumpIt is the best for acquisition but... our platform Stardust is the also best for analysis!
Access it on https://my.comae.com - info@comae.com if you have any questions.

  Destination path:           \??\C:\Users\Cindy\Documents\Comae-Toolkit-3.0.20190919.1\x64\CASEY-20191002-173332.dmp

  Computer name:              CASEY


  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.18362
  MachineId:                   218C6415-2182-4D7B-AA91-7554B0D7ACC1
  TimeStamp:                   132145112156437950
  Cr3:                         0x1ad002
  KdCopyDataBlock:             0xfffff803412a2094
  KdDebuggerData:              0xfffff803414255e0
  KdpDataBlockEncoded:         0xfffff80341469378

  Current date/time:          [2019-10-02 (YYYY-MM-DD) 17:33:35 (UTC)]
  + Processing...
```

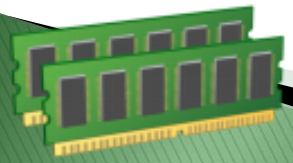


Dumpit.exe Cont'd

- Next open the .mem file created in a Hex Editor to view the memory dump and analyze the captured RAM contents.



215E4BAF0	20	74	6F	20	61	6C	70	68	61	20	63	6F	6D	70	6F	6E	to alpha compon
215E4BB00	65	6E	74	2E	00	00	00	00	00	00	00	00	00	00	00	00	ent.
215E4BB10	54	6F	6F	20	6D	61	6E	79	20	74	65	78	74	75	72	65	Too many texture
215E4BB20	20	61	64	64	72	65	73	73	69	6E	67	20	69	6E	73	74	addressing inst
215E4BB30	72	75	63	74	69	6F	6E	20	73	6C	6F	74	73	20	75	73	ruction slots us
215E4BB40	65	64	3A	20	25	64	2E	20	4D	61	78	2E	20	61	6C	6C	ed: %d. Max. all
215E4BB50	6F	77	65	64	20	69	73	20	25	64	2E	20	28	4E	6F	74	owed is %d. (Not
215E4BB60	65	20	74	68	61	74	20	73	6F	6D	65	20	74	65	78	74	e that some text
215E4BB70	75	72	65	20	61	64	64	72	65	73	73	69	6E	67	20	69	ure addressing i
215E4BB80	6E	73	74	72	75	63	74	69	6F	6E	73	20	6D	61	79	20	nstructions may
215E4BB90	75	73	65	20	75	70	20	6D	6F	72	65	20	74	68	61	6E	use up more than
215E4BBA0	20	6F	6E	65	20	69	6E	73	74	72	75	63	74	69	6F	6E	one instruction
215E4BBB0	20	73	6C	6F	74	29	00	00	00	00	00	00	00	00	00	00	slot)
215E4BBC0	54	6F	6F	20	6D	61	6E	79	20	61	72	69	74	68	6D	65	Too many arithme
215E4BBD0	74	69	63	20	69	6E	73	74	72	75	63	74	69	6F	6E	20	tic instruction
215E4BBE0	73	6C	6F	74	73	20	75	73	65	64	3A	20	25	64	2E	20	slots used: %d.
215E4BBF0	4D	61	78	2E	20	61	6C	6C	6F	77	65	64	20	28	63	6F	Max. allowed (co
215E4BC00	75	6E	74	69	6E	67	20	61	6E	79	20	63	6F	2D	69	73	unting any co-is
215E4BC10	73	75	65	64	20	70	61	69	72	73	20	61	73	20	31	29	sued pairs as 1)
215E4BC20	20	69	73	20	25	64	2E	00	00	00	00	00	00	00	00	00	is %d.
215E4BC30	54	6F	74	61	6C	20	6E	75	6D	62	65	72	20	6F	66	20	Total number of
215E4BC40	69	6E	73	74	72	75	63	74	69	6F	6E	20	73	6C	6F	74	instruction slot
215E4BC50	73	20	75	73	65	64	20	74	6F	6F	20	68	69	67	68	3A	s used too high:
215E4BC60	20	25	64	2E	20	4D	61	78	2E	20	61	6C	6C	6F	77	65	%d. Max. allowe
215E4BC70	64	20	28	63	6F	75	6E	74	69	6E	67	20	61	6E	79	20	d (counting any
215E4BC80	63	6F	2D	69	73	73	75	65	64	20	70	61	69	72	73	20	co-issued pairs
215E4BC90	61	73	20	31	29	20	69	73	20	25	64	2E	00	00	00	00	as 1) is %d.
215E4BCA0	72	30	20	6D	75	73	74	20	62	65	20	77	72	69	74	74	r0 must be writt



What can we find in memory?

HxD - [C:\Users\Cindy\Desktop\DumpIt\CASEY-20151223-231609.raw]

File Edit Search View Analysis Extras Window ?

16 ANSI hex

CASEY-20151223-231609.raw

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
1931D9410  73 73 32 30 31 20 53 2E 20 31 38 74 68 20 53 74  ss201 S. 18th St
1931D9420  72 65 65 74 2C 20 41 70 74 2E 20 36 32 30 00 05  reet, Apt. 620..
1931D9430  24 21 C7 40 78 08 00 05 24 21 C7 40 78 08 6E 47  $!Ç@x...$!Ç@x.nG
1931D9440  6A 5A 2B 47 57 61 53 66 61 46 72 5A 45 31 3A 93  jZ+GWaSfaFrZE1:"
1931D9450  4E 08 00 1B 23 09 06 06 2D 6B 65 79 77 6F 72 64  N...#...-keyword
1931D9460  69 74 20 73 65 63 75 72 69 74 79 00 05 24 21 C1  it security..$!Á
1931D9470  FF 12 28 00 05 24 21 C1 FF 12 28 2B 6D 57 59 59  ÿ.(..$!Áÿ.(+mWYY
1931D9480  73 63 41 53 55 61 73 75 37 4B 4C 44 93 4D 08 00  scASUasu7KLD"M..
1931D9490  2F 23 09 06 06 2D 73 65 61 72 63 68 62 61 72 2D  /#...-searchbar-
1931D94A0  68 69 73 74 6F 72 79 63 6F 6D 63 61 73 74 20 6D  historycomcast m
1931D94B0  69 6C 00 05 24 21 B4 98 87 68 00 05 24 21 B4 98  il..$!´˜‡h..$!´˜
1931D94C0  87 68 4D 43 57 44 68 63 76 6B 52 63 61 47 44 39  ‡hMCWDhcvkRcaGD9
1931D94D0  63 56 44 93 4C 08 00 1D 33 01 06 06 2D 55 73 65  cVD"L...3...-Use
1931D94E0  72 4E 61 6D 65 63 6C 63 61 73 65 79 40 63 6F 6D  rNameclcasey@com
1931D94F0  63 61 73 74 2E 6E 65 74 05 00 05 24 21 99 D9 BE  cast.net...$!™Ù¾
1931D9500  10 00 05 24 3A 9A 24 5D F8 48 47 6A 2B 6E 69 36  ...$:š$]øHGj+ni6
1931D9510  66 52 41 65 52 76 4A 4B 65 38 93 4B 08 00 1D 1D  fRAeRvJKe8"K....
1931D9520  09 06 06 2D 55 73 65 72 6E 61 6D 65 65 34 38 6D  ...-Username248j
1931D9530  78 6E 63 70 00 05 24 21 98 8B 87 78 00 05 24 21  xncp..$!˜‹‡x..$!
1931D9540  98 8B 87 78 70 64 4A 56 5A 57 62 75 51 65 4F 4D  ˜‹‡xpdJVZWbuQeOM
1931D9550  4D 41 62 58 4E 93 4A 08 00 33 33 09 06 06 2D 43  MAbXN"J..33...-C
1931D9560  6F 6E 66 69 72 6D 50 72 69 6D 61 72 79 45 6D 61  onfirmPrimaryEma
1931D9570  69 6C 63 6C 63 61 73 65 79 40 63 6F 6D 63 61 73  ilclcasey@comcas
1931D9580  74 2E 6E 65 74 00 05 24 21 98 8B 87 78 00 05 24  t.net..$!˜‹‡x..$
1931D9590  21 98 8B 87 78 58 35 35 52 72 42 72 59 54 39 4F  !˜‹‡xX55RrBrYT9O
1931D95A0  39 77 4E 53 51 47 93 49 08 00 25 33 09 06 06 2D  9wNSQG"I..%3...-
1931D95B0  50 72 69 6D 61 72 79 45 6D 61 69 6C 63 6C 63 61  PrimaryEmailclca
1931D95C0  73 65 79 40 63 6F 6D 63 61 73 74 2E 6E 65 74 00  sey@comcast.net.
1931D95D0  05 24 21 98 8B 87 78 00 05 24 21 98 8B 87 78 35  .$!˜‹‡x..$!˜‹‡x5
1931D95E0  51 68 72 6F 65 53 56 54 44 57 44 61 33 50 6A 3B  QhroeSVTDWDa3Pj;
1931D95F0  93 48 08 00 1B 23 01 06 06 2D 4B 65 79 77 6F 72  "H...#...-Keywor
1931D9600  64 49 54 20 53 65 63 75 72 69 74 79 02 00 05 24  dIT Security...$
1931D9610  21 7F AD 4D 90 00 05 24 22 0E 56 02 58 6F 5A 2F  !..M...$".V.XoZ/
1931D9620  79 66 48 66 48 51 44 36 6A 37 74 2F 56 4D 93 47  yfHfHQD6j7t/VM"G
1931D9630  08 00 2F 35 09 06 06 2D 73 65 61 72 63 68 62 61  ../5...-searchba
1931D9640  72 2D 68 69 73 74 6F 72 79 68 6F 77 20 74 6F 20  r-historyhow to
1931D9650  63 6F 64 65 20 69 6E 20 6D 79 73 71 6C 00 05 24  code in mysql..$
```

Offset: 1931D952C | Block: 1931D952C-1931D9533 | Length: 8 | Overwrite

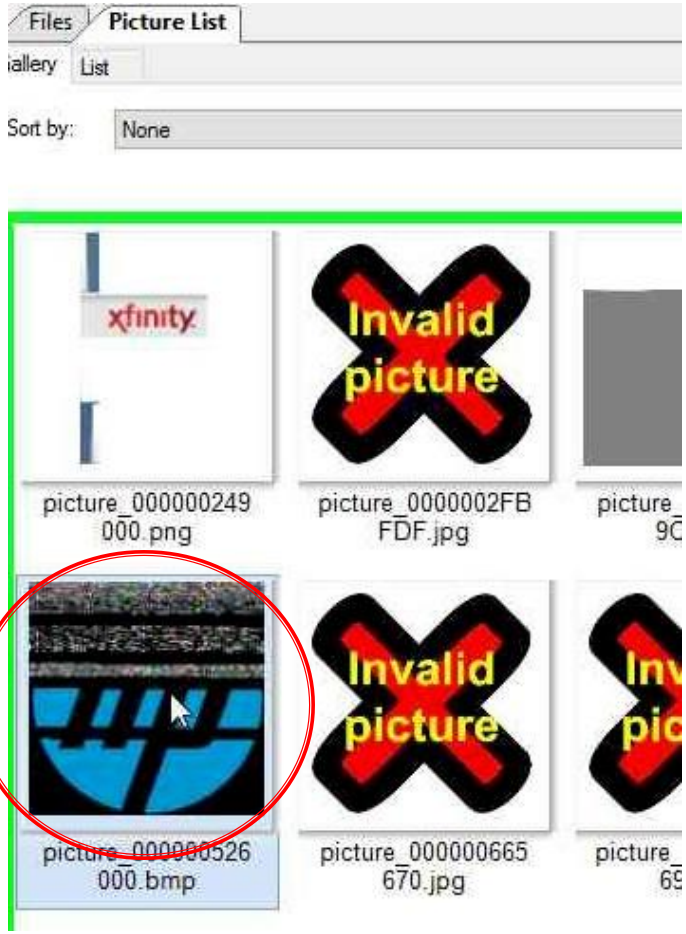
PayPal Email address

PayPal Account Password

These credentials were changed after this dump!

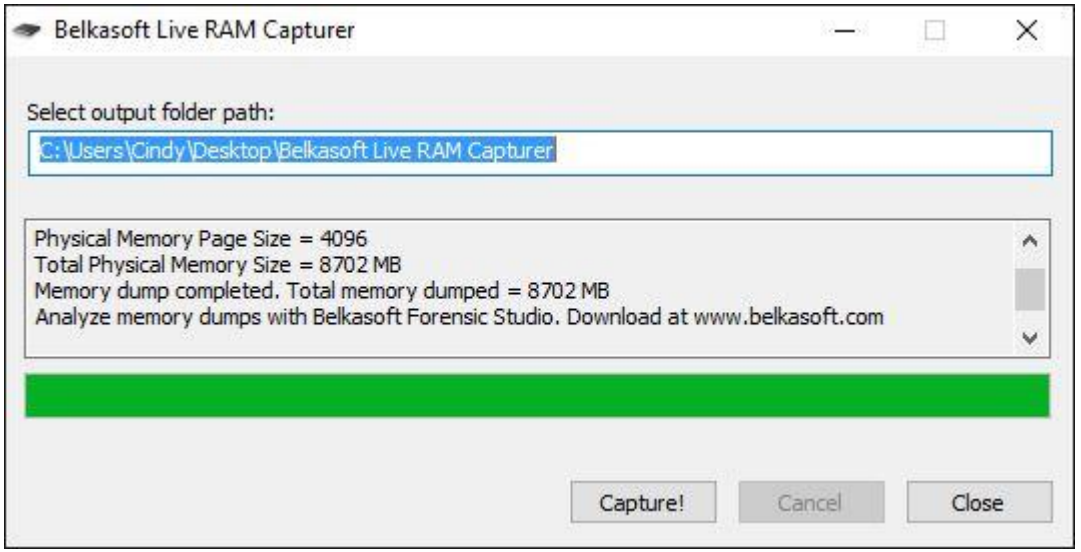
Using Belkasoft RAM Capturer

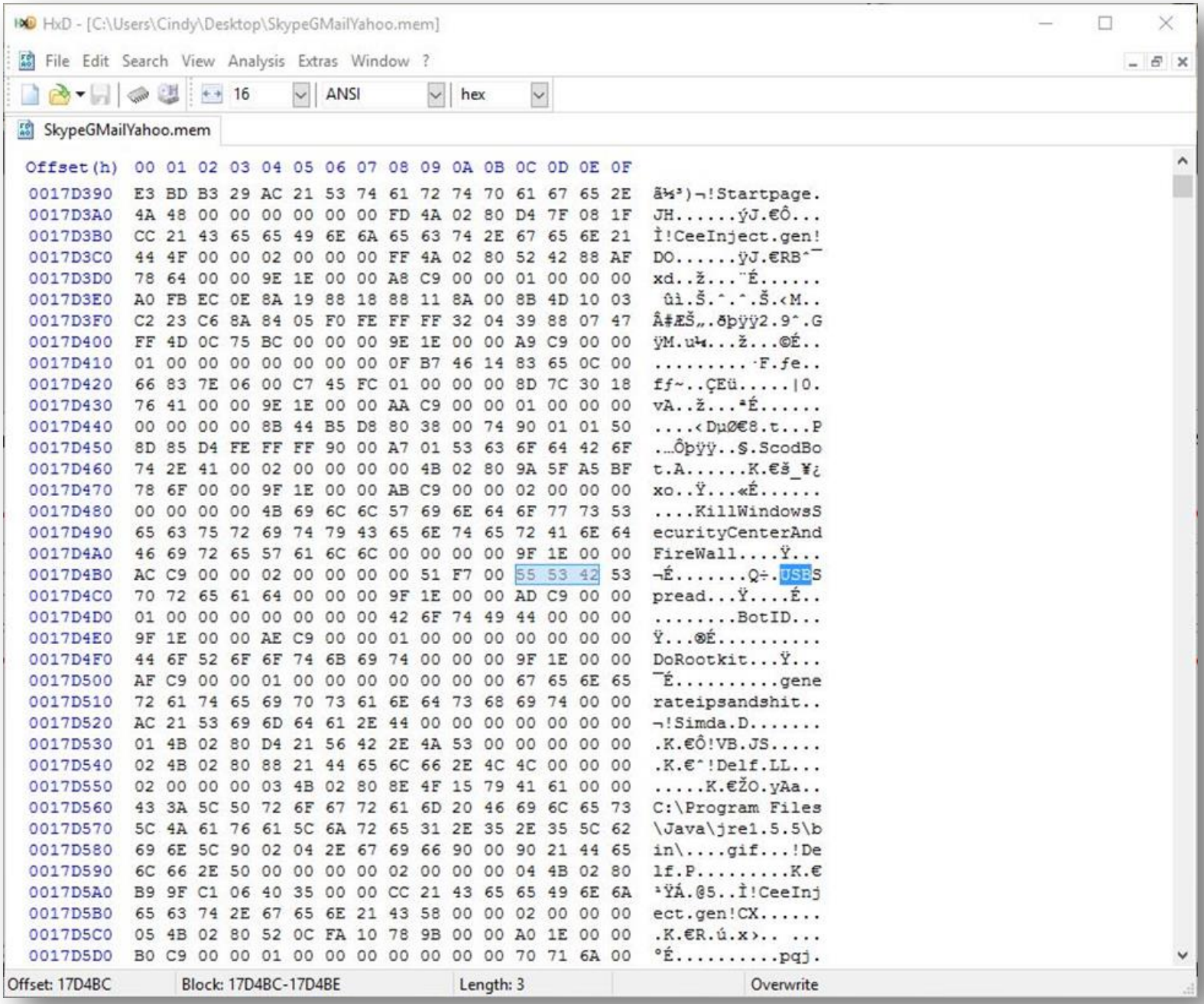
- RAM Images Show How Data Fades Away
  - ✓ Examining images retrieved from the memory dump demonstrates how RAM fades gradually over time.
  - ✓ Some studies have shown that RAM can be frozen for up to 10 minutes using a can of compressed air.

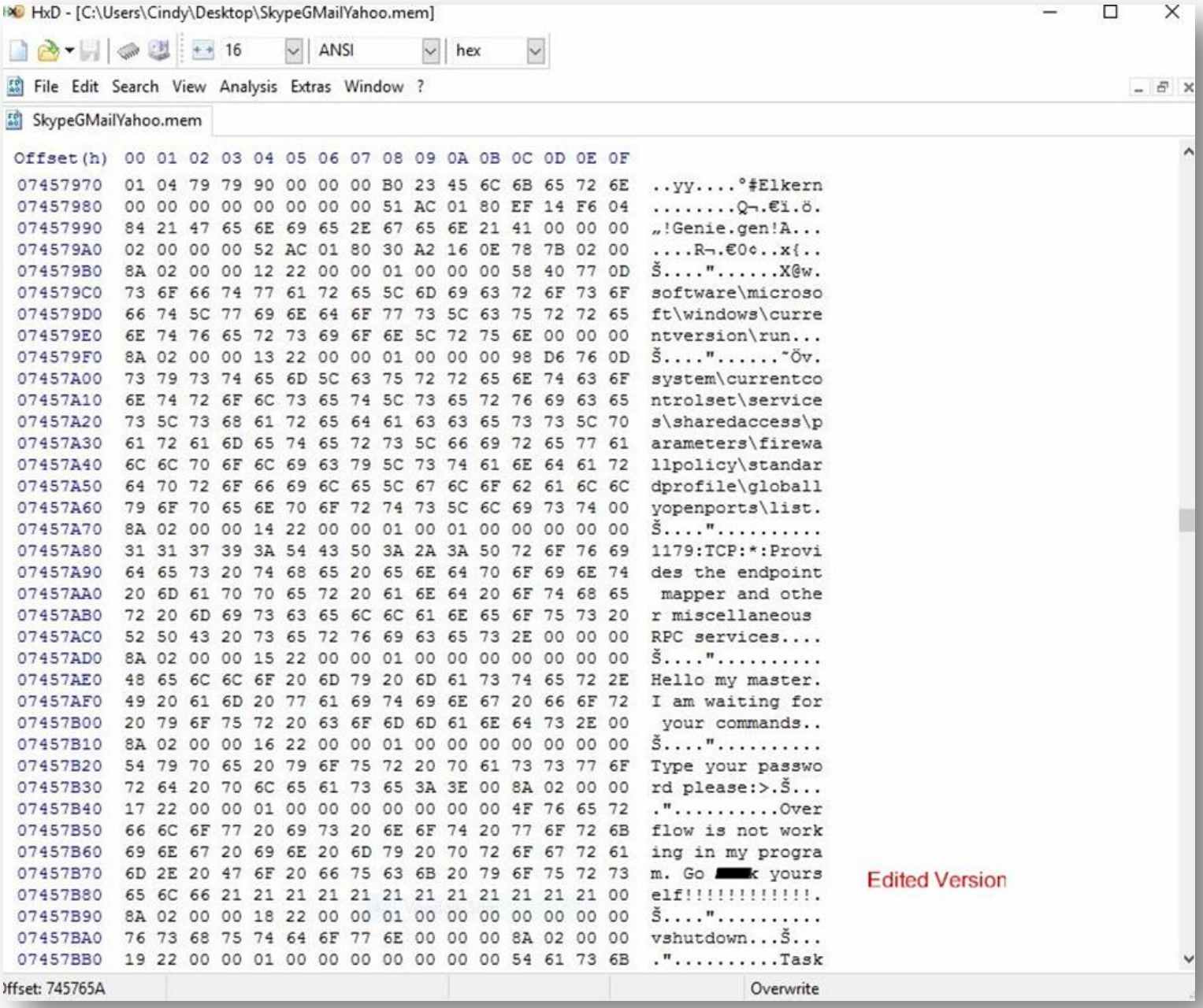


Belkasoft RAM Capturer

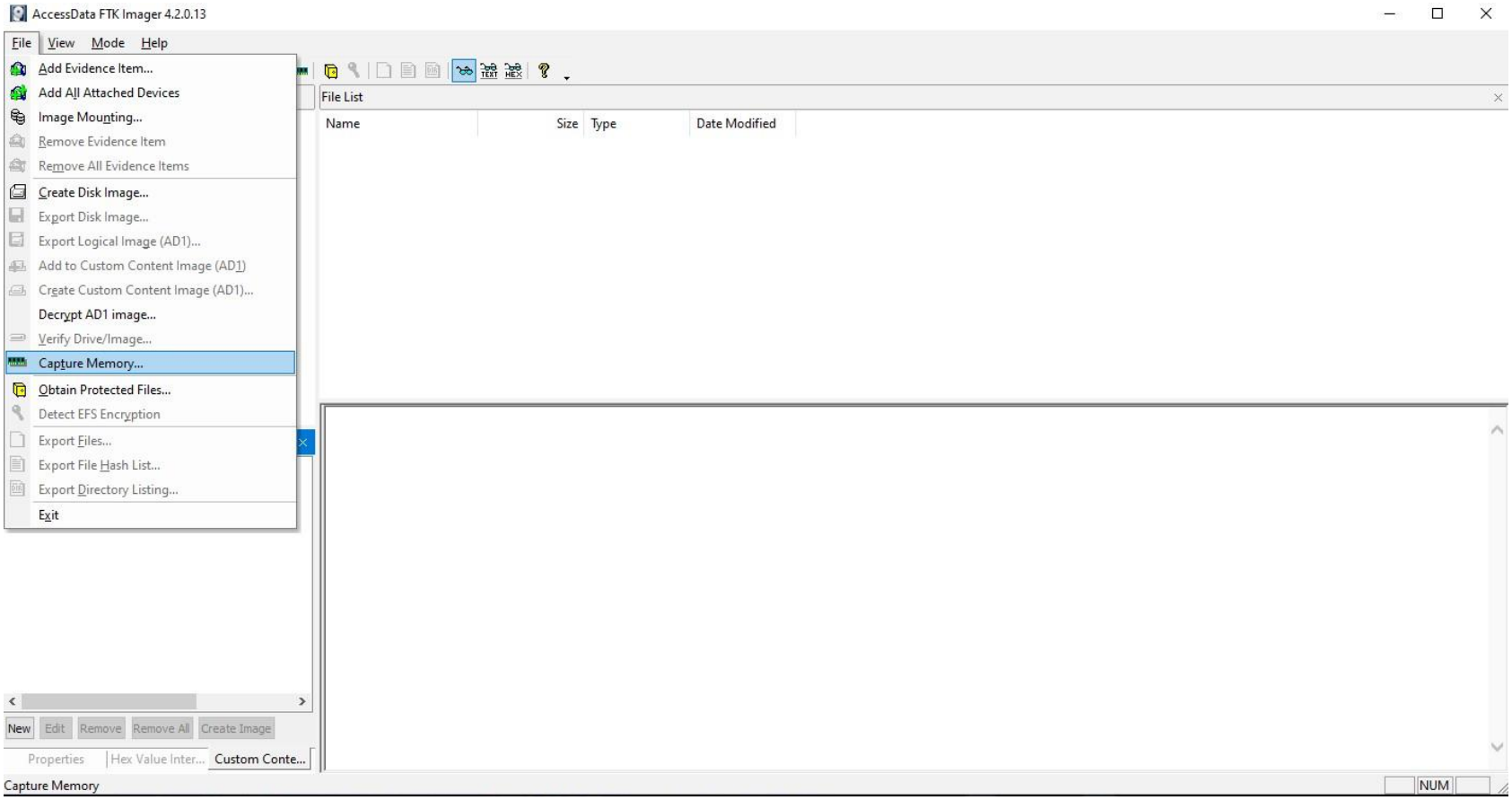
1. Open Belkasoft Live RAM Capturer and select “Capture!”.
2. When the process is complete, close the application.
3. Open the .mem file you just created with Hex Editor.

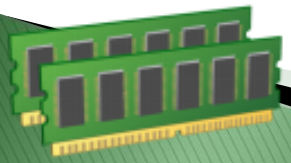



HxD - [C:\Users\Cindy\Desktop\SkypeGMailYahoo.mem]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
SkypeGMailYahoo.mem
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0017D390 E3 BD B3 29 AC 21 53 74 61 72 74 70 61 67 65 2E ã½³)¬!Startpage.
0017D3A0 4A 48 00 00 00 00 00 00 FD 4A 02 80 D4 7F 08 1F JH......ýJ.€Ô...
0017D3B0 CC 21 43 65 65 49 6E 6A 65 63 74 2E 67 65 6E 21 Ì!CeeInject.gen!
0017D3C0 44 4F 00 00 02 00 00 00 FF 4A 02 80 52 42 88 AF DO......ÿJ.€RBˆ¯
0017D3D0 78 64 00 00 9E 1E 00 00 A8 C9 00 00 01 00 00 00 xd..ž...¨É......
0017D3E0 A0 FB EC 0E 8A 19 88 18 88 11 8A 00 8B 4D 10 03 ûì.Š.ˆ.ˆ.Š.‹M..
0017D3F0 C2 23 C6 8A 84 05 F0 FE FF FF 32 04 39 88 07 47 Â#ÆŠ„.ðþÿÿ2.9ˆ.G
0017D400 FF 4D 0C 75 BC 00 00 00 9E 1E 00 00 A9 C9 00 00 ÿM.u¼...ž...©É..
0017D410 01 00 00 00 00 00 00 00 0F B7 46 14 83 65 0C 00 ....·F.ƒe..
0017D420 66 83 7E 06 00 C7 45 FC 01 00 00 00 8D 7C 30 18 fƒ~..ÇEü.....|0.
0017D430 76 41 00 00 9E 1E 00 00 AA C9 00 00 01 00 00 00 vA..ž...ªÉ......
0017D440 00 00 00 00 8B 44 B5 D8 80 38 00 74 90 01 01 50 ....‹DµØ€8.t...P
0017D450 8D 85 D4 FE FF FF 90 00 A7 01 53 63 6F 64 42 6F ..Ôþÿÿ..§.ScodBo
0017D460 74 2E 41 00 02 00 00 00 00 4B 02 80 9A 5F A5 BF t.A......K.€š_¥¿
0017D470 78 6F 00 00 9F 1E 00 00 AB C9 00 00 02 00 00 00 xo..Ÿ...«É......
0017D480 00 00 00 00 4B 69 6C 6C 57 69 6E 64 6F 77 73 53 ....KillWindowsS
0017D490 65 63 75 72 69 74 79 43 65 6E 74 65 72 41 6E 64 ecurityCenterAnd
0017D4A0 46 69 72 65 57 61 6C 6C 00 00 00 00 9F 1E 00 00 FireWall....Ÿ...
0017D4B0 AC C9 00 00 02 00 00 00 00 51 F7 00 55 53 42 53 ¬É.......Q÷.USBS
0017D4C0 70 72 65 61 64 00 00 00 9F 1E 00 00 AD C9 00 00 pread...Ÿ....É..
0017D4D0 01 00 00 00 00 00 00 00 42 6F 74 49 44 00 00 00 ....BotID...
0017D4E0 9F 1E 00 00 AE C9 00 00 01 00 00 00 00 00 00 00 Ÿ...®É..........
0017D4F0 44 6F 52 6F 6F 74 6B 69 74 00 00 00 9F 1E 00 00 DoRootkit...Ÿ...
0017D500 AF C9 00 00 01 00 00 00 00 00 00 00 67 65 6E 65 ¯É..........gene
0017D510 72 61 74 65 69 70 73 61 6E 64 73 68 69 74 00 00 rateipsandshit..
0017D520 AC 21 53 69 6D 64 61 2E 44 00 00 00 00 00 00 00 ¬!Simda.D.......
0017D530 01 4B 02 80 D4 21 56 42 2E 4A 53 00 00 00 00 00 .K.€Ô!VB.JS.....
0017D540 02 4B 02 80 88 21 44 65 6C 66 2E 4C 4C 00 00 00 .K.€ˆ!Delf.LL...
0017D550 02 00 00 00 03 4B 02 80 8E 4F 15 79 41 61 00 00 .....K.€ŽO.yAa..
0017D560 43 3A 5C 50 72 6F 67 72 61 6D 20 46 69 6C 65 73 C:\Program Files
0017D570 5C 4A 61 76 61 5C 6A 72 65 31 2E 35 2E 35 5C 62 \Java\jre1.5.5\b
0017D580 69 6E 5C 90 02 04 2E 67 69 66 90 00 90 21 44 65 in\....gif...!De
0017D590 6C 66 2E 50 00 00 00 00 02 00 00 00 04 4B 02 80 lf.P.........K.€
0017D5A0 B9 9F C1 06 40 35 00 00 CC 21 43 65 65 49 6E 6A ¹ŸÁ.@5..Ì!CeeInj
0017D5B0 65 63 74 2E 67 65 6E 21 43 58 00 00 02 00 00 00 ect.gen!CX......
0017D5C0 05 4B 02 80 52 0C FA 10 78 9B 00 00 A0 1E 00 00 .K.€R.ú.x›.. ...
0017D5D0 B0 C9 00 00 01 00 00 00 00 00 00 00 70 71 6A 00 °É..........pqj.
Offset: 17D4BC
Block: 17D4BC-17D4BE
Length: 3
Overwrite

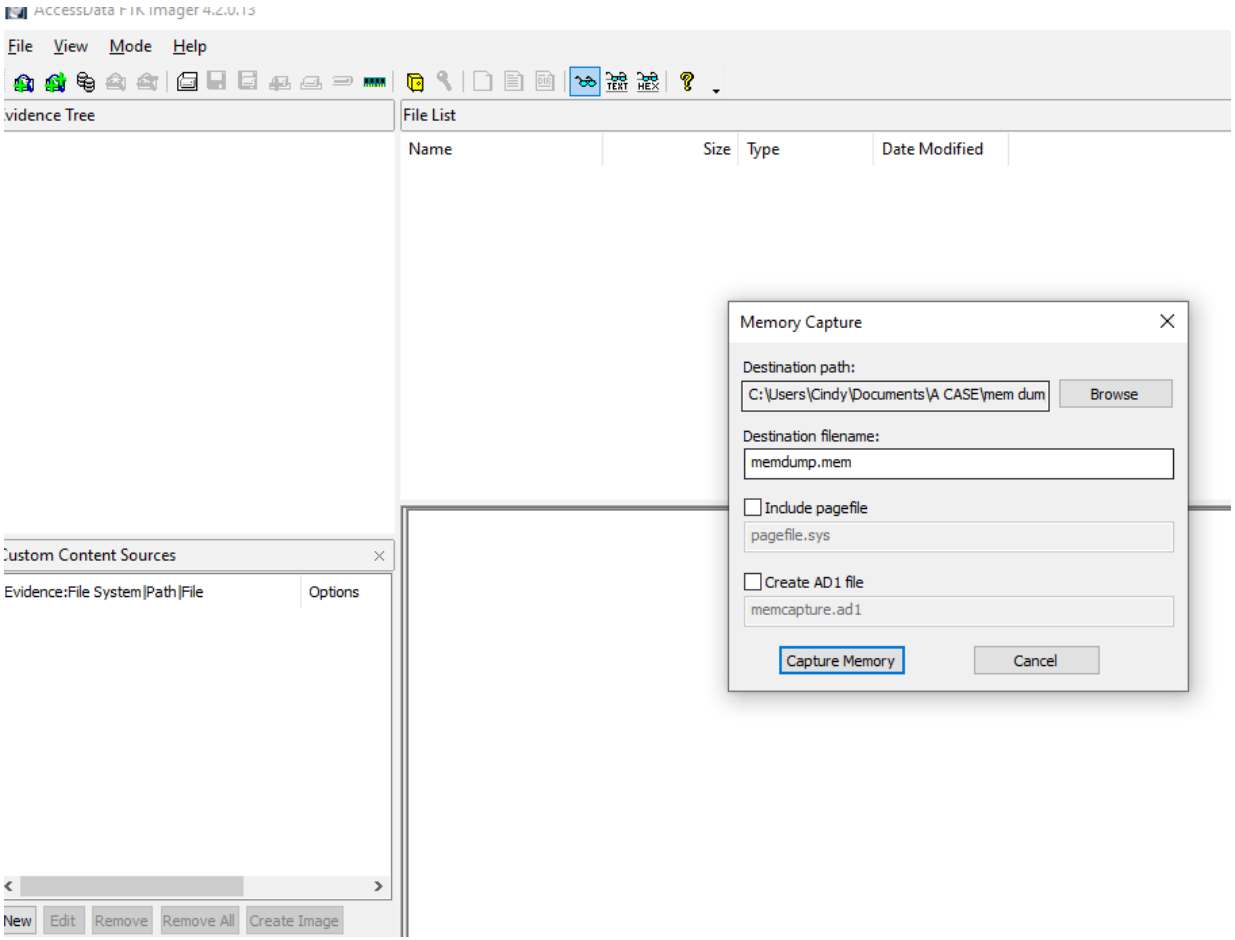

HxD - [C:\Users\Cindy\Desktop\SkypeGMailYahoo.mem]
16
ANSI
hex
File Edit Search View Analysis Extras Window ?
SkypeGMailYahoo.mem
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
07457970 01 04 79 79 90 00 00 00 B0 23 45 6C 6B 65 72 6E ..yy....°#Elkern
07457980 00 00 00 00 00 00 00 00 51 AC 01 80 EF 14 F6 04 ....Q¬.€ï.ö.
07457990 84 21 47 65 6E 69 65 2E 67 65 6E 21 41 00 00 00 „!Genie.gen!A...
074579A0 02 00 00 00 52 AC 01 80 30 A2 16 0E 78 7B 02 00 ....R¬.€0¢..x{..
074579B0 8A 02 00 00 12 22 00 00 01 00 00 00 58 40 77 0D Š....".....X@w.
074579C0 73 6F 66 74 77 61 72 65 5C 6D 69 63 72 6F 73 6F software\microso
074579D0 66 74 5C 77 69 6E 64 6F 77 73 5C 63 75 72 72 65 ft\windows\curre
074579E0 6E 74 76 65 72 73 69 6F 6E 5C 72 75 6E 00 00 00 ntversion\run...
074579F0 8A 02 00 00 13 22 00 00 01 00 00 00 98 D6 76 0D Š....".....˜Öv.
07457A00 73 79 73 74 65 6D 5C 63 75 72 72 65 6E 74 63 6F system\currentco
07457A10 6E 74 72 6F 6C 73 65 74 5C 73 65 72 76 69 63 65 ntrolset\service
07457A20 73 5C 73 68 61 72 65 64 61 63 63 65 73 73 5C 70 s\sharedaccess\p
07457A30 61 72 61 6D 65 74 65 72 73 5C 66 69 72 65 77 61 arameters\firewa
07457A40 6C 6C 70 6F 6C 69 63 79 5C 73 74 61 6E 64 61 72 llpolicy\standar
07457A50 64 70 72 6F 66 69 6C 65 5C 67 6C 6F 62 61 6C 6C dprofile\globall
07457A60 79 6F 70 65 6E 70 6F 72 74 73 5C 6C 69 73 74 00 yopenports\list.
07457A70 8A 02 00 00 14 22 00 00 01 00 01 00 00 00 00 00 Š....".........
07457A80 31 31 37 39 3A 54 43 50 3A 2A 3A 50 72 6F 76 69 1179:TCP:*:Provi
07457A90 64 65 73 20 74 68 65 20 65 6E 64 70 6F 69 6E 74 des the endpoint
07457AA0 20 6D 61 70 70 65 72 20 61 6E 64 20 6F 74 68 65 mapper and othe
07457AB0 72 20 6D 69 73 63 65 6C 6C 61 6E 65 6F 75 73 20 r miscellaneous
07457AC0 52 50 43 20 73 65 72 76 69 63 65 73 2E 00 00 00 RPC services....
07457AD0 8A 02 00 00 15 22 00 00 01 00 00 00 00 00 00 00 Š....".........
07457AE0 48 65 6C 6C 6F 20 6D 79 20 6D 61 73 74 65 72 2E Hello my master.
07457AF0 49 20 61 6D 20 77 61 69 74 69 6E 67 20 66 6F 72 I am waiting for
07457B00 20 79 6F 75 72 20 63 6F 6D 6D 61 6E 64 73 2E 00 your commands..
07457B10 8A 02 00 00 16 22 00 00 01 00 00 00 00 00 00 00 Š....".........
07457B20 54 79 70 65 20 79 6F 75 72 20 70 61 73 73 77 6F Type your passwo
07457B30 72 64 20 70 6C 65 61 73 65 3A 3E 00 8A 02 00 00 rd please:>.Š...
07457B40 17 22 00 00 01 00 00 00 00 00 00 00 4F 76 65 72 .".........Over
07457B50 66 6C 6F 77 20 69 73 20 6E 6F 74 20 77 6F 72 6B flow is not work
07457B60 69 6E 67 20 69 6E 20 6D 79 20 70 72 6F 67 72 61 ing in my progra
07457B70 6D 2E 20 47 6F 20 66 75 63 6B 20 79 6F 75 72 73 m. Go [redacted]k yours
07457B80 65 6C 66 21 21 21 21 21 21 21 21 21 21 21 21 00 elf!!!!!!!!!!!!.
07457B90 8A 02 00 00 18 22 00 00 01 00 00 00 00 00 00 00 Š....".........
07457BA0 76 73 68 75 74 64 6F 77 6E 00 00 00 8A 02 00 00 vshutdown...Š...
07457BB0 19 22 00 00 01 00 00 00 00 00 00 00 54 61 73 6B .".........Task
Edited Version
Offset: 745765A
Overwrite

FTK Imager

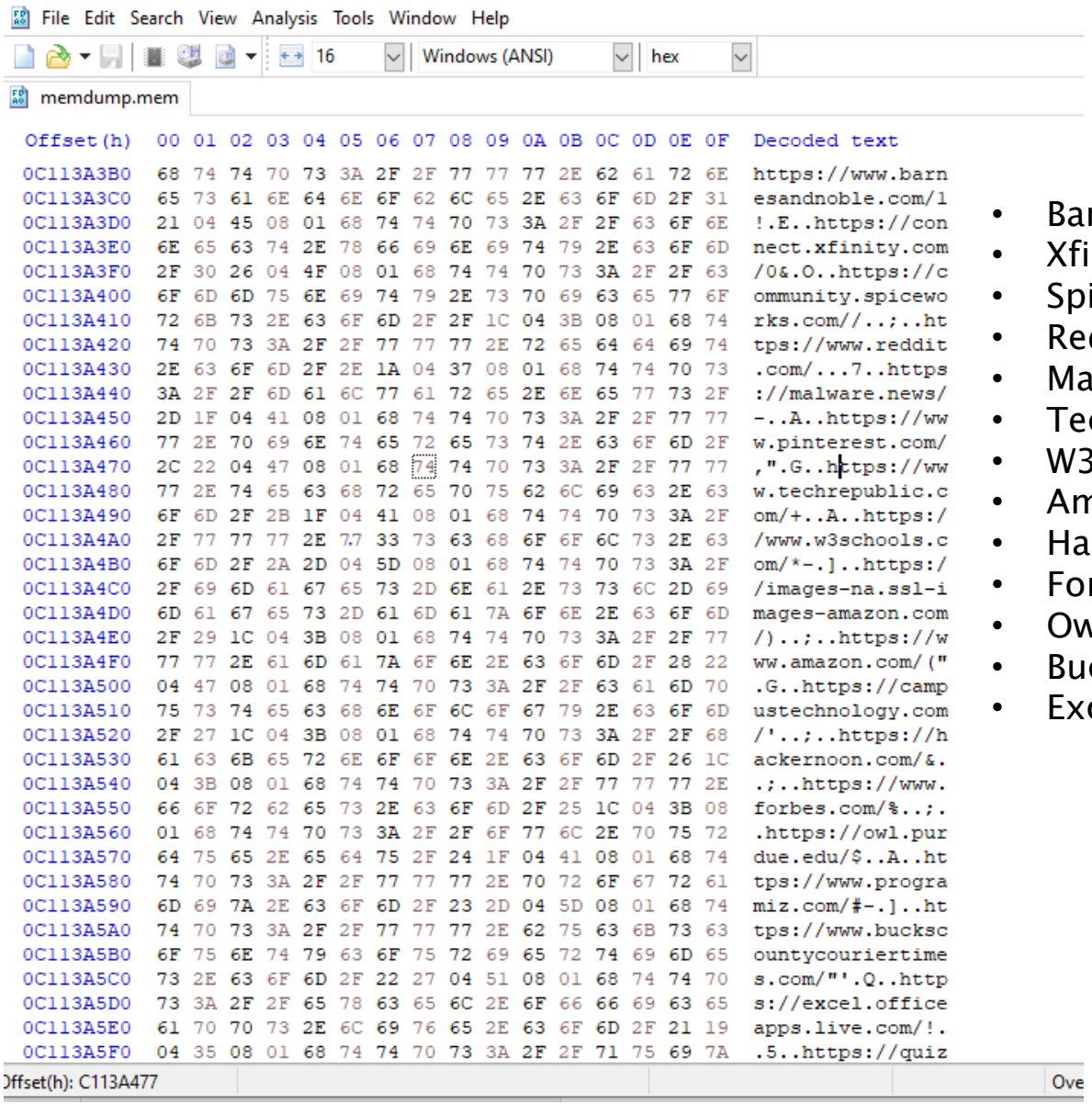

AccessData FTK Imager 4.2.0.13
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name
Size
Type
Date Modified
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
Capture Memory
NUM



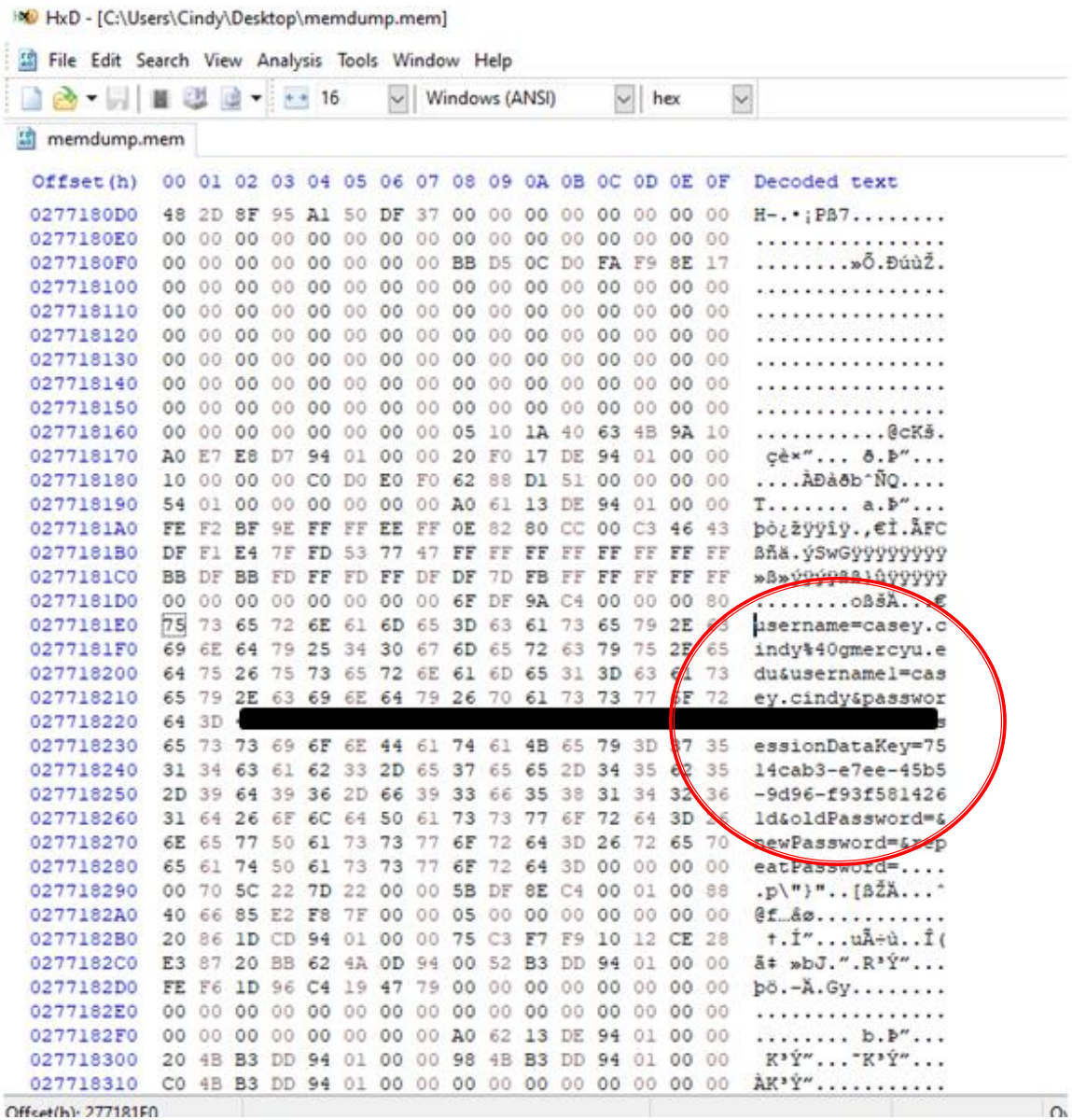
FTK Imager


AccessData FTK Imager 4.2.0.13
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Memory Capture
Destination path:
C:\Users\Cindy\Documents\A CASE\mem dum
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel

Web Browsing History



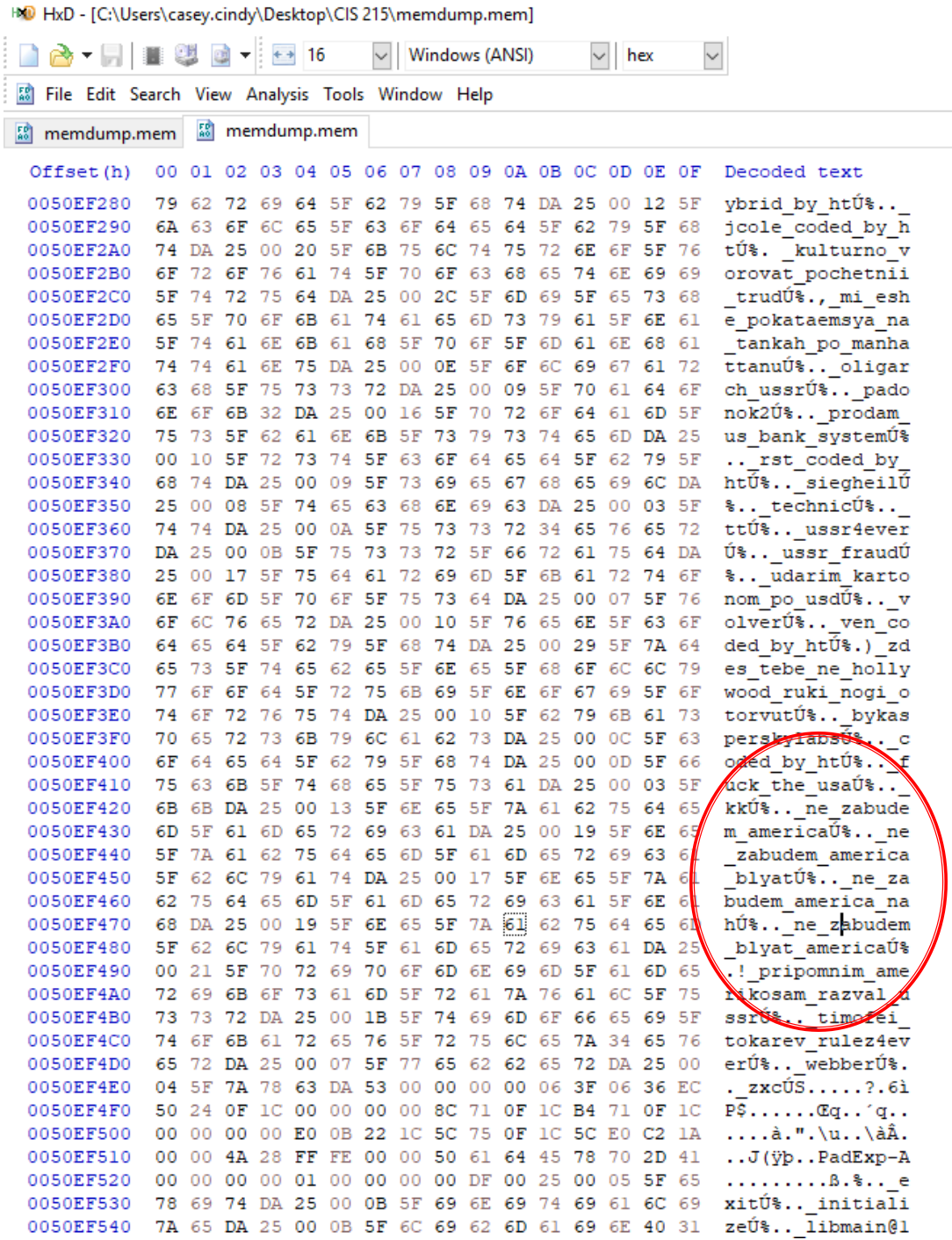
- Barnes and Noble
- Xfinity Email
- Spice Works
- Reddit
- Malware News
- Tech Republic
- W3Schools
- Amazon
- Hacker Noon
- Forbes
- Owl Purdue
- Bucks County Courier Times
- Excel Office Apps



Login Credentials

memdump.mem

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
02F77C360  3B 01 00 69 8B D7 68 8B 6C 24 20 FF 15 BC 34 01  ;..i‹×h‹l$ ÿ.¼4.
02F77C370  00 68 8B CF FF 15 73 3B 01 00 21 23 48 53 54 52  .h‹Ïÿ.s;..!#HSTR
02F77C380  3A 4C 61 6E 67 75 61 67 65 2E 46 72 65 6E 63 68  :Language.French
02F77C390  2E 41 00 02 00 00 00 EF 71 00 10 4A E3 37 C9 61  .A.....ïq..Jã7Éa
02F77C3A0  8E 00 00 C5 65 5A 90 33 12 53 7B 56 C8 48 7C FE  Ž..ÅeZ.3.S{VÈH|þ
02F77C3B0  3B 7B E5 1E AA AB 4D 6C 65 20 73 65 72 76 65 75  ;{å.ª«Mle serveu
02F77C3C0  72 20 64 65 20 6D 69 73 65 73 6A 6F 75 72 20 64  r de misesjour d
02F77C3D0  65 20 64 69 73 70 6F 6E 69 62 6C 65 6D 65 72 63  e disponiblemerc
02F77C3E0  69 20 64 65 20 6E 6F 75 73 6C 69 67 6E 65 20 6F  i de nousligne o
02F77C3F0  63 63 75 70 61 6E 74 6C 00 65 00 20 00 70 00 72  ccupantl.e. .p.r
02F77C400  00 6F 00 67 00 72 00 61 00 6D 00 6D 00 65 00 20  .o.g.r.a.m.m.e.
02F77C410  00 64 00 27 00 69 00 6E 00 73 00 74 00 61 00 6C  .d.'.i.n.s.t.a.l
02F77C420  00 6C 00 61 00 74 00 69 00 6F 00 6E 00 21 23 48  .l.a.t.i.o.n.!#H
02F77C430  53 54 52 3A 42 61 63 6B 64 6F 6F 72 3A 57 69 6E  STR:Backdoor:Win
02F77C440  33 32 2F 41 6C 75 6D 69 6E 75 6D 41 70 74 21 6C  32/AluminumApt!l
02F77C450  6F 77 66 69 00 02 00 00 00 F0 71 00 10 69 77 8E  owfi.....ðq..iwŽ
02F77C460  16 61 80 00 00 6E FB 99 38 C5 FE 3C 32 B7 6F 90  .a€..nû™8Åþ<2·o.
02F77C470  6E 13 06 99 92 17 E1 9D 7A 69 20 61 6D 20 76 69  n..™'.á.zi am vi
02F77C480  72 75 73 21 20 66 75 63 6B 20 79 6F 75 20 3A 2D  rus! [redacted] you :-
02F77C490  29 77 69 6C 6C 20 75 6E 69 6E 73 74 61 6C 6C 20  )will uninstall
02F77C4A0  73 65 72 76 69 63 65 2C 73 75 72 65 3F 20 2D 3A  service,sure? -:
02F77C4B0  29 69 6E 70 75 74 20 74 68 65 20 61 64 64 72 65  )input the addre
02F77C4C0  73 73 20 77 68 69 63 68 20 77 69 6C 6C 20 61 63  ss which will ac
02F77C4D0  63 65 73 73 28 6F 66 66 2D 6C 69 6E 65 20 6B 65  cess(off-line ke
02F77C4E0  79 6C 6F 67 21 23 50 55 41 3A 42 75 6E 64 6C 65  ylog!#PUA:Bundle
02F77C4F0  72 43 6C 75 73 74 65 72 3A 49 64 6D 32 00 02 00  rCluster:Idm2...
02F77C500  00 00 F1 71 00 10 66 1B 18 3C 61 8E 00 00 32 A5  ..ñq..f..<aŽ..2¥
02F77C510  FC EA 45 5D 26 87 46 56 E0 D0 6B 00 C1 C8 2F 33  üêE]&‡FVàÐk.ÁÈ/3
02F77C520  16 F2 61 6C 73 6F 20 76 65 72 69 66 79 20 74 68  .òalso verify th
02F77C530  61 74 20 69 64 6D 20 69 6E 74 65 67 72 61 74 69  at idm integrati
02F77C540  6F 6E 20 69 6E 74 6F 20 79 6F 75 72 20 62 72 6F  on into your bro
02F77C550  77 73 65 72 20 69 73 20 74 75 72 6E 65 64 20 6F  wser is turned o
02F77C560  6E 20 69 6E 20 69 64 6D 20 6F 70 74 69 6F 6E 73  n in idm options
```



не забудем америка
не забудем америка
блять не развал усср
тимофей токарев
рулез4евр веббер

we will not forget America we will not forget America f@#!ing do not collapse ussr timofey tokarev rulez4evr

About 1,950,000,000 results (0.60 seconds)

Russian ⇄ English

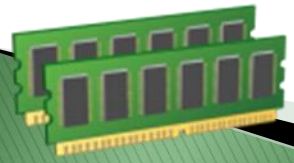
покатаемся на танках по манхаттан олигарх усср

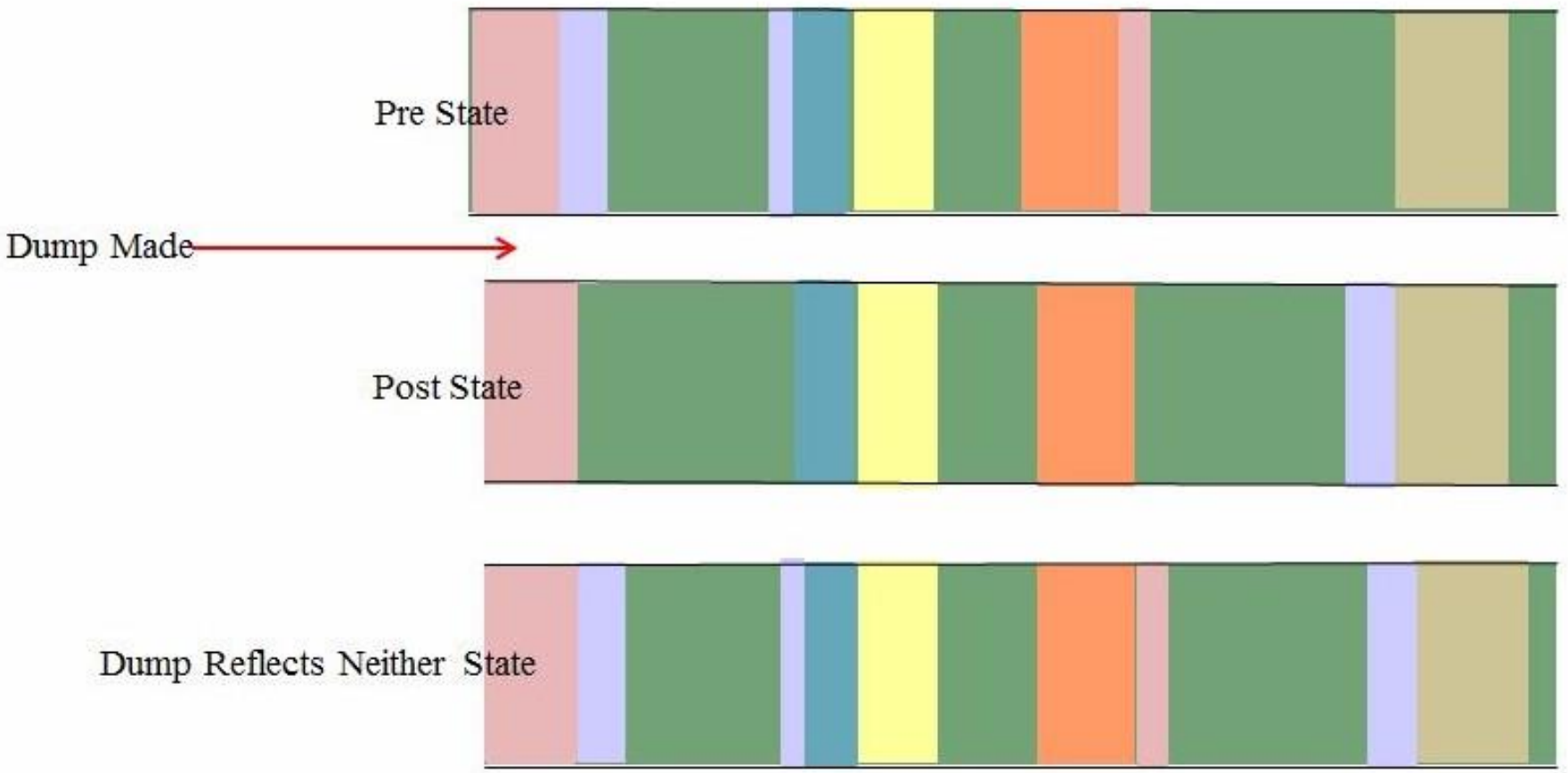
pokatayemsya na tankakh po mankhattan oligarkh ussr

ride tanks on manhattan oligarch ussr

Challenges

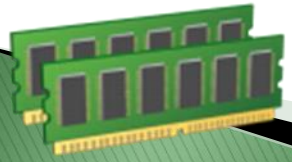
- Volatile memory (RAM) is in constant flux.
  - Time sliding window
- Creating a RAM dump changes the evidence.
  - No write-block.
- Image cannot be validated.
  - Pre and post MD5, SHA- 1, SHA-256 hashes useless.
- Can be difficult to explain in laymen terms.




Pre State
Dump Made
Post State
Dump Reflects Neither State

Closing Thoughts…

- The types of cases I am going to do don't involve this stuff – *How will you know?*
- RAM imaging is *going* to be industry standard - it's just a matter of time.
- Machine may have a Rootkit - *Ever hear of Sony*?
- I will just use FTK – *Not enough*



Questions?