DFRWS 2023 Challenge

– DFRWS 2023 Challenge on Industrial Control System Forensics –

"The Troubled Elevator: Forensic Investigation of a Bank's Elevator Malfunctioning"

Authors

Md Ashiqur Rahman (mdrahman@augusta.edu)
Dr. Gokila Dorai (gdorai@augusta.edu)

Augusta University

June 2024

Contents

Introduction

The DFRWS 2023 challenge is about the domain of Industrial Control Systems (ICS), specifically focusing on programmable logic controllers (PLC). These systems are increasingly critical for monitoring and controlling industrial processes in various sectors, such as energy, water, transportation, and manufacturing. Despite their importance, advancements in security and forensics have not been adequate. This challenge seeks to offer more profound understanding of ICS network traffic and device memory analysis in practical settings.

The scenario for this challenge, “The Troubled Elevator,” involves investigating a mysterious incident in a bank’s executive-only elevator. To overcome this DFRWS challenge difficulty, we have investigated at four different levels.

1. **Visual Footage Analysis:** The CCTV footage depicts the entire session of the elevator malfunctioning. The video demonstrates the points of abnormalities observed in different timestamps.

2. **Device Level Analysis:** Two types of devices are analyzed with various tools to identify the presence of malicious programs. Here, we attempted to follow the trail of any undesirable actions that might have contributed to this unprecedented occurrence. We have examined following artifacts in this stage.

   a. PC Memory
   b. PLC Internal and External Memory

3. **Network Level Analysis:** The network activities are closely examined to identify the presence of suspicious participants and classify if any alteration has been made.

4. **Accumulation of individual level findings:** In this stage we corelate several findings from different aspects and expose patterns of potential interest.

1.1 Challenge Scenario

Kristi Wayne from Wayne Enterprise has recently bought a controversial bank in the city of Richmond. On June 29, Friday afternoon, during her visit to the bank, she used an executive-only elevator designed to provide a smooth and private commute for the high-ranking officials within the bank. Wayne enters the elevator and presses the button to get to another floor. However, the elevator suddenly starts malfunctioning, trapping Wayne inside. Wayne calls from the elevator for emergency assistance. After an extended episode of patience and misery, she is finally rescued. The elevator infrastructure is designed to log network traffic and device memory dumps for a certain time-period. The CCTV footage of the elevator and the memory dump of Wayne's new computer in her office at the bank are also acquired.

1.2 Challenge Questions

The objective of this challenge is to investigate the entire incident and provide a comprehensive report, including:

- Elevator behaviors during malfunctioning
- Timeline of elevator malfunctioning
- Specific cause of malfunctioning
- Any evidence of an inside attacker
- Any attack evidence on the network, computer, and PLC device

1.3 Accumulated Artifacts

Following artifacts are collected from the scene and labeled accordingly:

1. (**A1**) CCTV footage of the elevator.
2. (**A2**) Memory dump of Kristi Waynes's computer.
3. (**A3**) Network diagram.
4. (**A4**) Network traffic log of the elevator's PLC.
5. (**A5**) 7 External PLC Memory dumps.
6. (**A6**) 7 On-Chip PLC Memory dumps.
7. (**A7**) PLC control logic manual.
8. (**A8**) Elevator manual.

1.4 Concept Diagram

The overall network architecture is given in figure 1. The scenario depicts the connectivity among the computers and the associated devices.

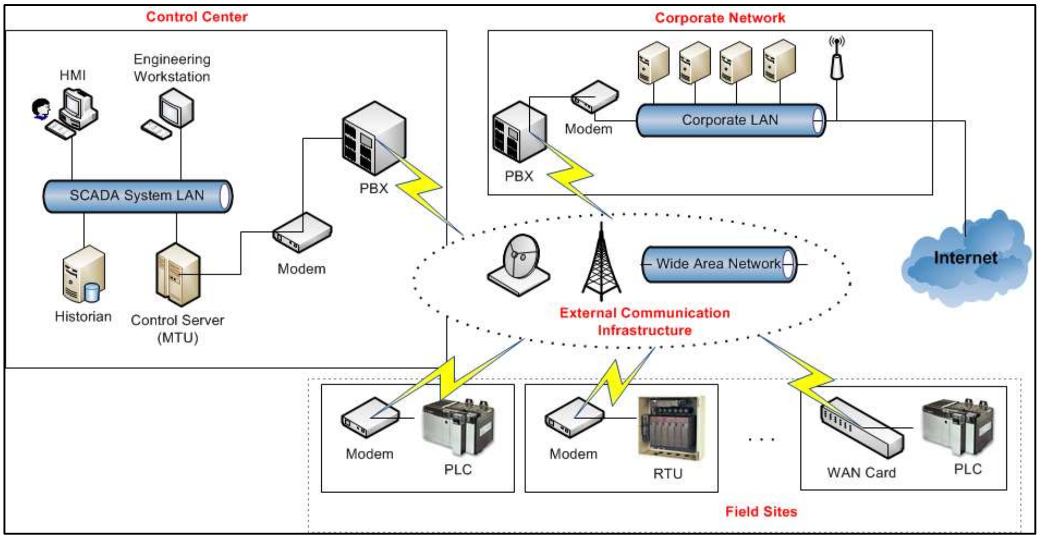


Figure 1: Overall network schema of the scenario

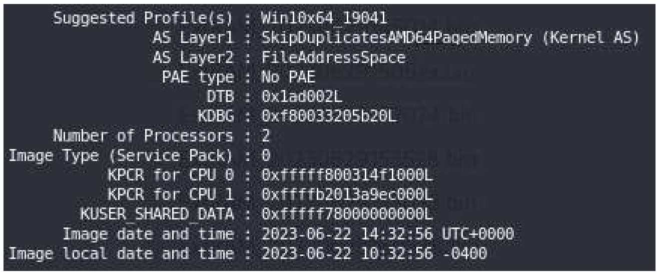
Overview of Challenge Data

2.1 (A1) CCTV footage of the elevator

A CCTV footage of the elevator of the size of 380.9 MB in “mp4” format is given. The duration of the video is 01:17:21 hrs. The timestamp analysis and the findings are described in section 3.1.

2.2 (A2) Memory dump of Kristi Wayne’s computer

A memory dump of the PC in binary format has been provided with the size of 2.1 GB. The preliminary investigation shows that, “DumpIT” by “Magnet Corporation” has been used as the memory acquisition tool. The memory dump shows that, the artifact has been collected from a PC of “Windows” operating system in figure 2 (extracted using Volatality v 2 KBG imagemap). Extensive analysis has been conducted and illustrated on section 3.2.



```
     Suggested Profile(s) : Win10x64_19041
                AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                AS Layer2 : FileAddressSpace
                 PAE type : No PAE
                      DTB : 0x1ad002L
                     KDBG : 0xf80033205b20L
     Number of Processors : 2
Image Type (Service Pack) : 0
           KPCR for CPU 0 : 0xfffff800314f1000L
           KPCR for CPU 1 : 0xffffb2013a9ec000L
        KUSER_SHARED_DATA : 0xfffff78000000000L
      Image date and time : 2023-06-22 14:32:56 UTC+0000
Image local date and time : 2023-06-22 10:32:56 -0400
```

Figure 2: Operating System of the PC Memory Dump

2.3 (A3) Network diagram

A network diagram has been provided describing the topology and the IP addresses of the connected devices. This diagram in figure 3 demonstrates the connections of the workstations, HMI, Log server and the PLC host (elevator).

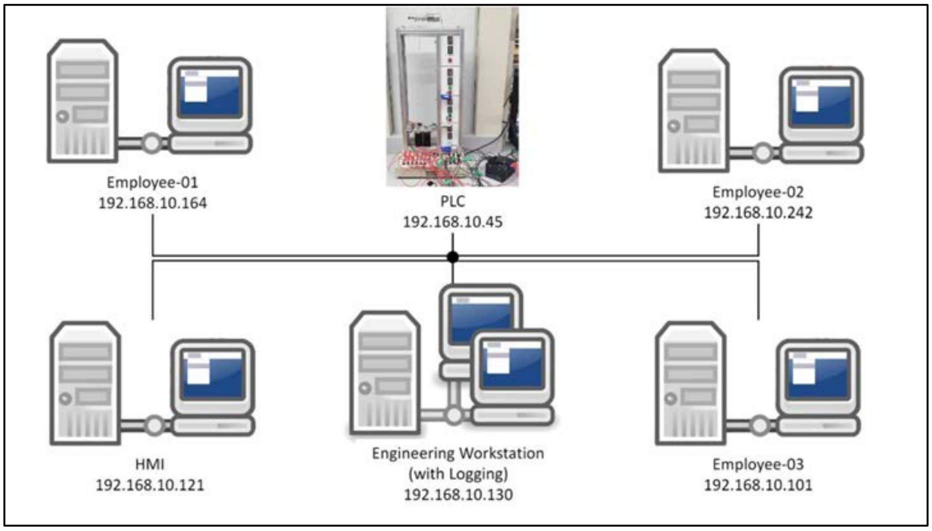


Figure 3: The network

2.4 (A4) Network traffic log of the elevator's PLC

A network traffic log of the elevator's PLC has been provided in "pcapng" format of size 30.6 MB. We have examined this file with our own developed program, Wireshark, and Network Miner. The findings are explained in section 3.3.

2.5 (A5) (A6) PLC device memory dumps

Here two types of binary files are given: 1) (A5) ExtMemoryRAM, and 2) (A6) InChipRAM of size 524.3 KB and 131.1 KB respectively. Each category contains 7 memory dump files with 7 consecutive timestamps in order. We tried to extract useful information and forensic evidence available in these files and explained in section 3.4.

2.6 (A7) PLC control logic manual

There is a PLC control logic handbook available that details the elevator PLC's model number. Modicon M221 (TM221C16R) by Schneider Electric with Ethernet module has been used in this experiment as defined in figure 4. Though the PLC is equipped with a Serial line, is this challenge, all communication has been conducted using Modbus TCP protocol.

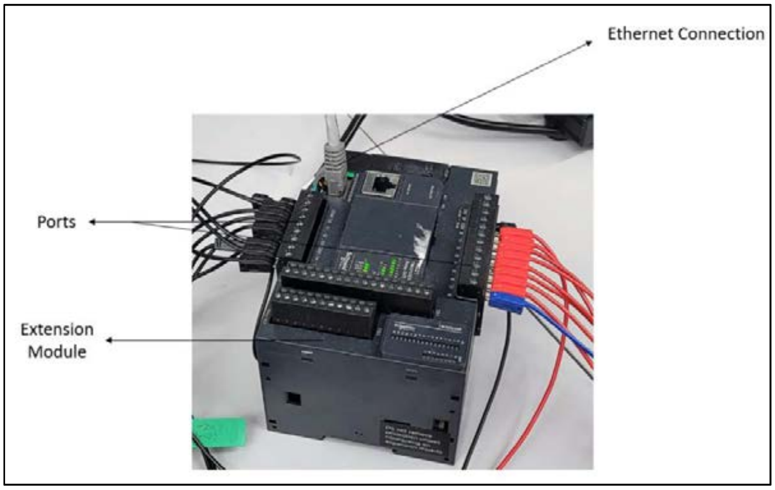


Figure 4: Modicon M221 PLC

2.7 (A8) Elevator manual

This challenge is also facilitated with an elevator manual where the system configuration of the elevator is explained with great details. Figure 5 shows the experimental testbed of the scenario with the elevator and the PLC module.

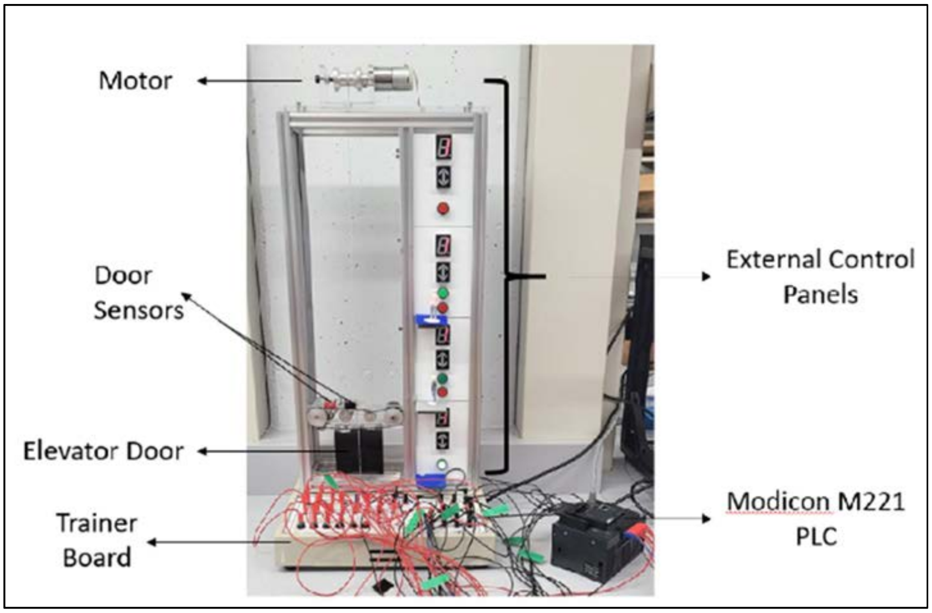


Figure 5: Experimental setup of the elevator with Modicon PLC

Forensic Analysis

3.1 (A1) CCTV footage analysis

Software used: VLC player

We have analyzed the CCTV footage and manually labeled the different stages of the elevator. We have identified 6 important marker in the video: 1) Door (Open/ Closed), 2) Passenger (Onboard/ None), 3) Lights of each floor (Red/ Green/ Off), 4) Floor Display, 5) Elevator's Direction (Up/ Down/ Both/ Off), and 6) Manual Involvement (1,2,3,4,R – Reset, B - Broken). An unknown/ non-accepted state is labeled with *. The figure 6 represents all states of the elevator that are shown in the video.

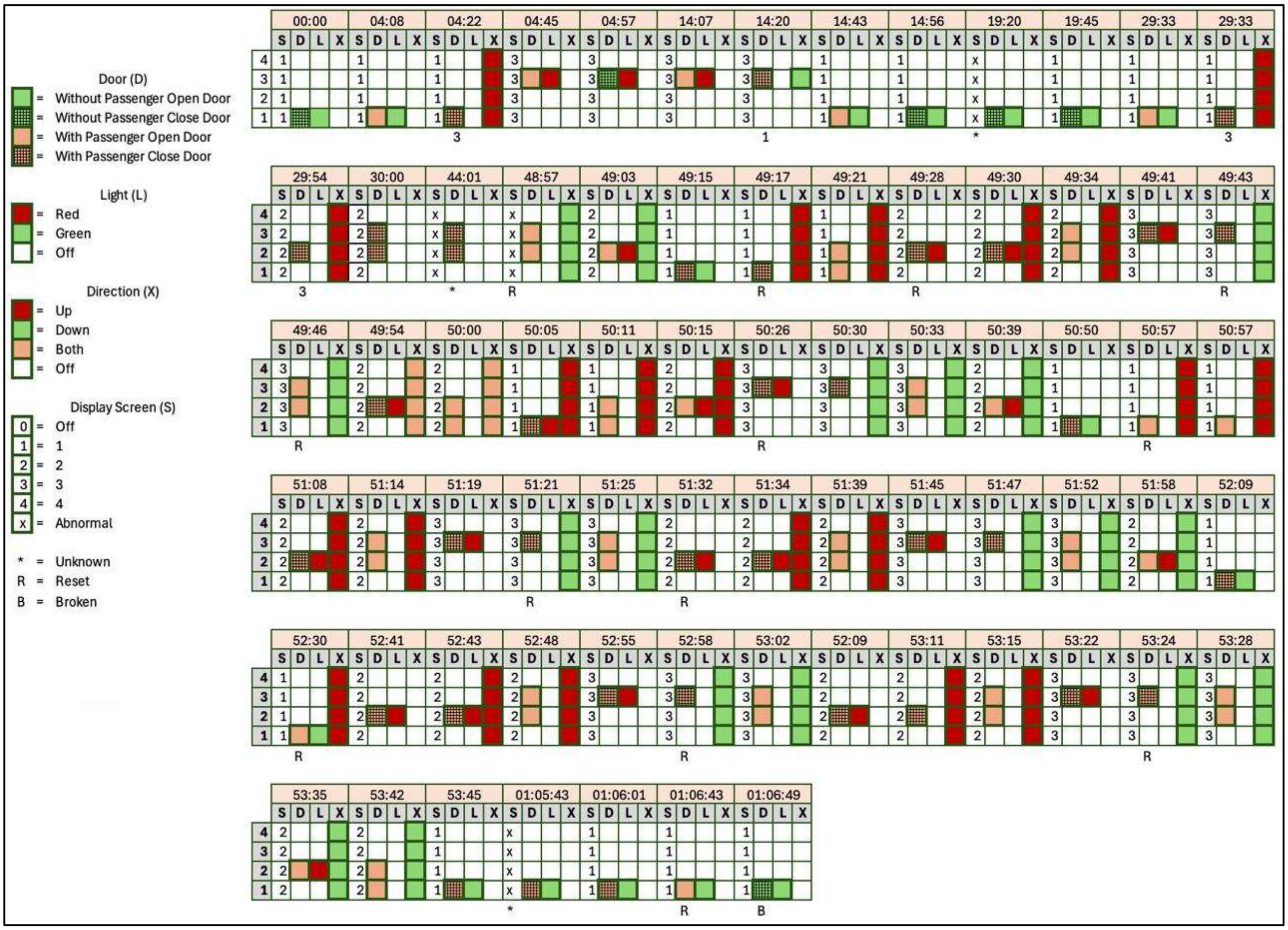


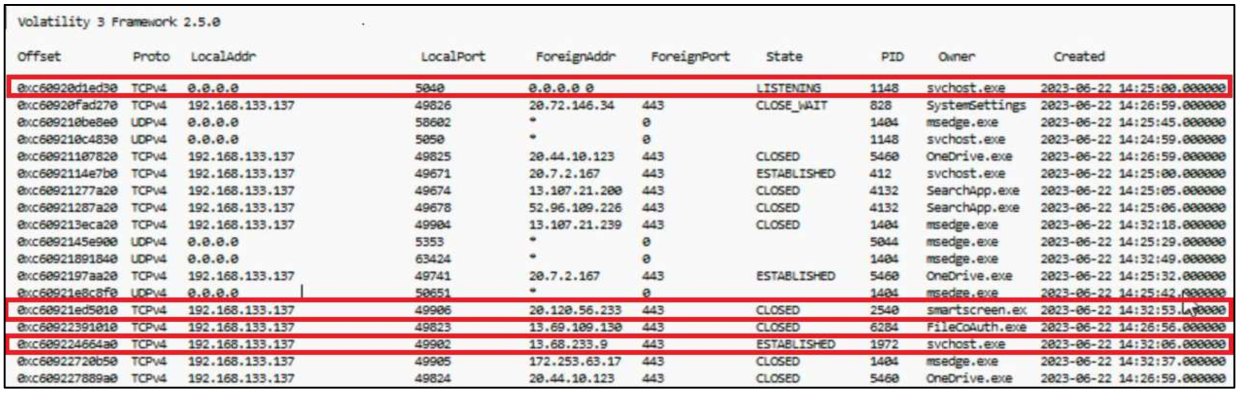
Figure 6: State representation of the elevator.

The figure also demonstrates the timeline of elevator malfunctioning. We have noticed unrecognized markers labeled as "x" in the elevator floor displays at 19:20, 44:01, and 01:05:43. We assume the exploitation on the elevator's PLC module has been accomplished before 19:20.

3.2 (A2) PC Memory dump analysis

Software used: Volatility 2, Volatility 3, Autopsy, Gidra, PE Studio, Bulk Extractor (Kali Linux), REMNUX tools, HxD, Bless, Wireshark, Network Miner.

Analysis 1: We have used both Volatility version 2 and 3 to find the Process lists, Process tree, Registry Hives, Network status etc. We found the host IP address is 192.168.133.137 as defined in figure 7; whereas the network diagram shows the IP address of Kristi Waynes's computer is 192.168.10.145.

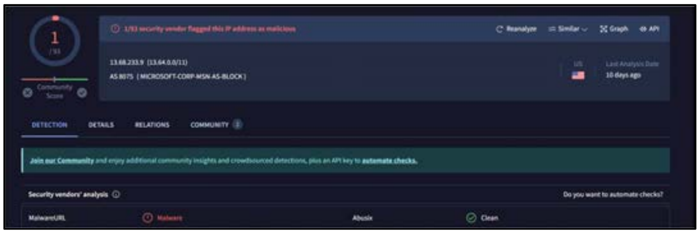


```
Volatility 3 Framework 2.5.0

Offset          Proto   LocalAddr          LocalPort   ForeignAddr     ForeignPort   State         PID    Owner             Created

0xc60920d1ed30  TCPv4   0.0.0.0            5040        0.0.0.0 0                     LISTENING     1148   svchost.exe       2023-06-22 14:25:00.000000
0xc60920fad270  TCPv4   192.168.133.137    49826       20.72.146.34    443           CLOSE_WAIT    828    SystemSettings    2023-06-22 14:26:59.000000
0xc609210be8e0  UDPv4   0.0.0.0            58602       *               0                           1404   msedge.exe        2023-06-22 14:25:45.000000
0xc609210c4830  UDPv4   0.0.0.0            5050        *               0                           1148   svchost.exe       2023-06-22 14:24:59.000000
0xc60921107820  TCPv4   192.168.133.137    49825       20.44.10.123    443           CLOSED        5460   OneDrive.exe      2023-06-22 14:26:59.000000
0xc6092114e7b0  TCPv4   192.168.133.137    49671       20.7.2.167      443           ESTABLISHED   412    svchost.exe       2023-06-22 14:25:00.000000
0xc60921277a20  TCPv4   192.168.133.137    49674       13.107.21.200   443           CLOSED        4132   SearchApp.exe     2023-06-22 14:25:05.000000
0xc60921287a20  TCPv4   192.168.133.137    49678       52.96.109.226   443           CLOSED        4132   SearchApp.exe     2023-06-22 14:25:06.000000
0xc609213eca20  TCPv4   192.168.133.137    49904       13.107.21.239   443           CLOSED        1404   msedge.exe        2023-06-22 14:32:18.000000
0xc6092145e900  UDPv4   0.0.0.0            5353        *               0                           5044   msedge.exe        2023-06-22 14:25:29.000000
0xc60921891840  UDPv4   0.0.0.0            63424       *               0                           1404   msedge.exe        2023-06-22 14:32:49.000000
0xc6092197aa20  TCPv4   192.168.133.137    49741       20.7.2.167      443           ESTABLISHED   5460   OneDrive.exe      2023-06-22 14:25:32.000000
0xc60921e8c8f0  UDPv4   0.0.0.0            50651       *               0                           1404   msedge.exe        2023-06-22 14:25:42.000000
0xc60921ed5010  TCPv4   192.168.133.137    49906       20.120.56.233   443           CLOSED        2540   smartscreen.ex    2023-06-22 14:32:53.000000
0xc60922391010  TCPv4   192.168.133.137    49823       13.69.109.130   443           CLOSED        6284   FileCoAuth.exe    2023-06-22 14:26:56.000000
0xc609224664a0  TCPv4   192.168.133.137    49902       13.68.233.9     443           ESTABLISHED   1972   svchost.exe       2023-06-22 14:32:06.000000
0xc60922720b50  TCPv4   192.168.133.137    49905       172.253.63.17   443           CLOSED        1404   msedge.exe        2023-06-22 14:32:37.000000
0xc609227889a0  TCPv4   192.168.133.137    49824       20.44.10.123    443           CLOSED        5460   OneDrive.exe      2023-06-22 14:26:59.000000
```

Figure 7: Volatality "netscan" output

Here we found 3 jobs (PID: 1148 svchost.exe; PID: 1972 svchost.exe; PID: 2540) with suspicious activities. Further analysis like "pstree/ psscan" on these jobs, do not provide any significant information.

Findings: According to "Virus Total" the "Foreign IP Address" 13.68.233.9 is suspicious, as defined in figure 8.



1/93 security vendor flagged this IP address as malicious

13.68.233.9 (13.64.0.0/11)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)

US
Last Analysis Date
10 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis
Do you want to automate checks?

MalwareURL Malware Abusix Clean

Figure 8: Suspicious Foreign IP

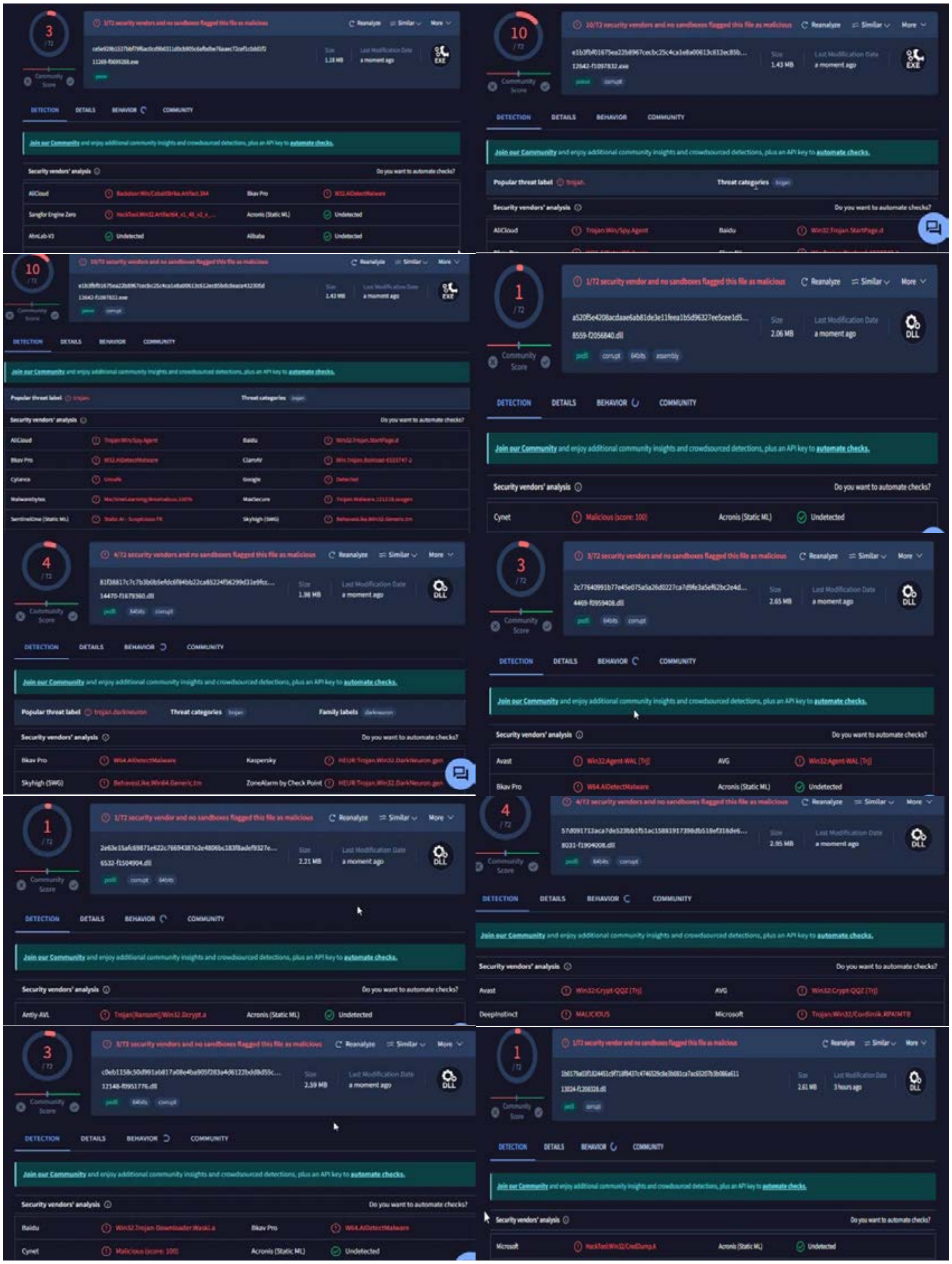
Analysis 2: We have used Autopsy to analyze the PC dumps further. Autopsy also recovered 15751 deleted files from the memory dump. Table 1 shows the extracted artifacts from the dump file.

In Memory Files		
	Artifact Type	**# of files extracted**
File Views	Image	142
	Audio	1
	Archives	15
	Database	23
Documents	HTML	13
	MS Office	2
	Plain Texts	1250
Executables	.exe	242
	.dll	1347
Application	x-dosexec	180
	vnd-ms-excel	1
	x-font-ttf	4
	x-msdownload	1471
	x-elc	1
	xml	24
	xhtml	2
	octet-stream	12303
	x-windows-registry	14
	ms-word	1
	x-sqlite3	23
	x-gzip	15
Audio	vnd-wave	1
Image	vnd-microsoft.icon	1
	x-portable-graymap	1
	png	137
	jpeg	5
	svg	1
	x-portable-pixmap	1
Text	x-java-source	189
	x-fortan	4
	plain	1251
	x-chdr	58
	xml	50
	csv	5
	x-csrc	2
	html	18
	x-ini	3

Deleted Files	
File Types	**# of files recovered**
c	2
csv	5
dat	1
dll	1369
doc	1
excel	1
edb	6
exe	235
f	4
fat	2
font	4
gz	15
h	58
html	12
icon	1
ini	3
java	189
jpg	5
mft	12282
mui	34
pf	2
png	137
reg	14
shortcut	6
sqlite3	23
txt	1250
unknown	1
wav	1
xml	75

Table 1: Artifact extracted by Autopsy

We have analyzed several exe, dll files using HxD Hex Editor, PE Studio and Gidra, and found the presence of several Trojans, Malwares, Spywares, Ransomwares etc. as shown in figure 9.



3 /72

3/72 security vendors and no sandboxes flagged this file as malicious

ce5e029b1537bbf7ff6acbcd9b0311d0cb905c6afbdbe76aaec72caf1cbdd1f2

11269-f0695268.exe

peexe

Size 1.18 MB

Last Modification Date a moment ago

Security vendors' analysis

AliCloud	Backdoor:Win/CobaltStrike.Artifact.3H4	Bkav Pro	W32.AIDetectMalware
Sangfor Engine Zero	HackTool.Win32.Artifact64_v1_48_v2_x_...	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected

10 /72

10/72 security vendors and no sandboxes flagged this file as malicious

e1b3fbf01675ea22b8967cecbc25c4ca1e8a00613c612ec85b...

12642-f1097832.exe

peexe corrupt

Size 1.43 MB

Last Modification Date a moment ago

Popular threat label trojan.

Threat categories trojan

Security vendors' analysis

AliCloud	Trojan:Win/Spy.Agent	Baidu	Win32.Trojan.StartPage.d

10 /72

10/72 security vendors and no sandboxes flagged this file as malicious

e1b3fbf01675ea22b8967cecbc25c4ca1e8a00613c612ec85b6dcbeaca432305d

12642-f1097832.exe

peexe corrupt

Size 1.43 MB

Last Modification Date a moment ago

Popular threat label trojan.

Threat categories trojan

Security vendors' analysis

AliCloud	Trojan:Win/Spy.Agent	Baidu	Win32.Trojan.StartPage.d
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Botload-6533747-2
Cylance	Unsafe	Google	Detected
Malwarebytes	MachineLearning/Anomalous.100%	MaxSecure	Trojan.Malware.121218.susgen
SentinelOne (Static ML)	Static AI - Suspicious PE	Skyhigh (SWG)	BehavesLike.Win32.Generic.tm

1 /72

1/72 security vendor and no sandboxes flagged this file as malicious

a520f5e4208acdaae6ab81de3e11feea1b5d96327ee5cee1d5...

8559-f2056840.dll

pedll corrupt 64bits assembly

Size 2.06 MB

Last Modification Date a moment ago

Security vendors' analysis

Cynet	Malicious (score: 100)	Acronis (Static ML)	Undetected

4 /72

4/72 security vendors and no sandboxes flagged this file as malicious

81f38817c7c7b3b0b5efdc6f84bb22ca85224f56299d31e9fcc...

14470-f1679360.dll

pedll 64bits corrupt

Size 1.98 MB

Last Modification Date a moment ago

Popular threat label trojan.darkneuron

Threat categories trojan

Family labels darkneuron

Security vendors' analysis

Bkav Pro	W64.AIDetectMalware	Kaspersky	HEUR:Trojan.Win32.DarkNeuron.gen
Skyhigh (SWG)	BehavesLike.Win64.Generic.tm	ZoneAlarm by Check Point	HEUR:Trojan.Win32.DarkNeuron.gen

3 /72

3/72 security vendors and no sandboxes flagged this file as malicious

2c77640991b77e45e075a5a26d0227ca7d9fe3a5ef62bc2e4d...

4469-f0959408.dll

pedll 64bits corrupt

Size 2.65 MB

Last Modification Date a moment ago

Security vendors' analysis

Avast	Win32:Agent-WAL [Trj]	AVG	Win32:Agent-WAL [Trj]
Bkav Pro	W64.AIDetectMalware	Acronis (Static ML)	Undetected

1 /72

1/72 security vendor and no sandboxes flagged this file as malicious

2e63e15afc69871e622c76694387e2e4806bc183f8adef9327e...

6532-f1504904.dll

pedll corrupt 64bits

Size 2.21 MB

Last Modification Date a moment ago

Security vendors' analysis

Antiy-AVL	Trojan[Ransom]/Win32.Dcrypt.a	Acronis (Static ML)	Undetected

4 /72

4/72 security vendors and no sandboxes flagged this file as malicious

57d091712aca7de523bb1f51ac15881917398db518ef318de6...

8031-f1904008.dll

pedll 64bits corrupt

Size 2.95 MB

Last Modification Date a moment ago

Security vendors' analysis

Avast	Win32:Crypt-QQZ [Trj]	AVG	Win32:Crypt-QQZ [Trj]
DeepInstinct	MALICIOUS	Microsoft	Trojan:Win32/Cordimik.RPA!MTB

3 /72

3/72 security vendors and no sandboxes flagged this file as malicious

c0eb1158c50d991ab817a08e4ba905f283a4d6122bdd8d55c...

12148-f0951776.dll

pedll 64bits corrupt

Size 2.59 MB

Last Modification Date a moment ago

Security vendors' analysis

Baidu	Win32.Trojan-Downloader.Waski.a	Bkav Pro	W64.AIDetectMalware
Cynet	Malicious (score: 100)	Acronis (Static ML)	Undetected

1 /72

1/72 security vendor and no sandboxes flagged this file as malicious

1b6179a03f1824451c9f718f8437c4746529c8e3b081ca7ac65207b5b066a611

13024-f1208328.dll

pedll corrupt

Size 2.61 MB

Last Modification Date 3 hours ago

Security vendors' analysis

Microsoft	HackTool:Win32/CredDump.A	Acronis (Static ML)	Undetected

Reanalyze
Similar
More
Community Score
EXE
DLL
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Do you want to automate checks?

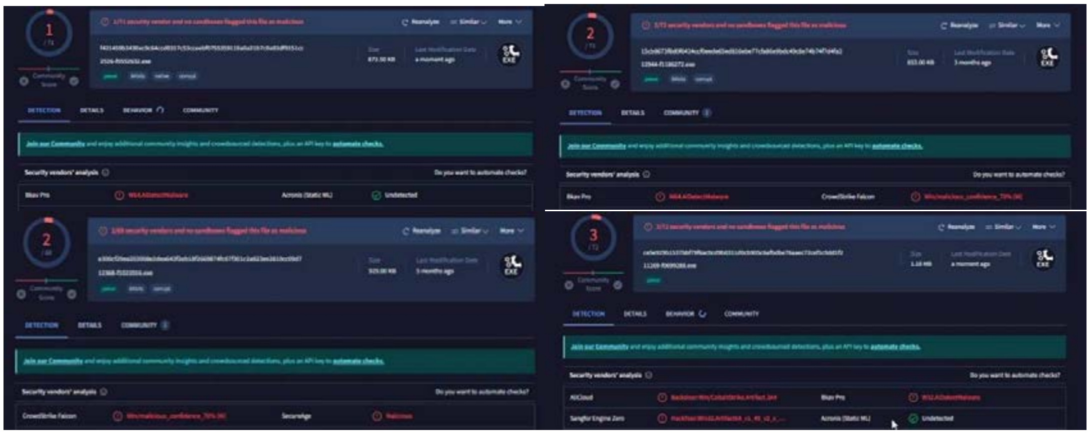
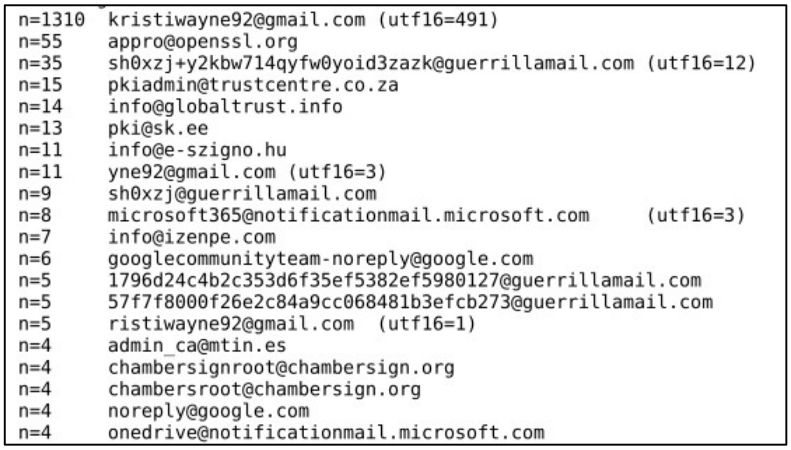


Figure 9: Presence of malicious files in PC Memory dump

Findings: As “Autopsy” is not able to extract the file creation time, it is not possible to trace the “dropper” software. The PC was intentionally infected by several malicious software, so that the footprint of the “dropper” software is not possible to identify.

Analysis 3: We have extracted 919 email address from the dump file. Based on the number of emails sent, figure 10 displays the top twenty email addresses. Here we found “kristiwayne92@gmail.com” email address has been accessed 1310 times.

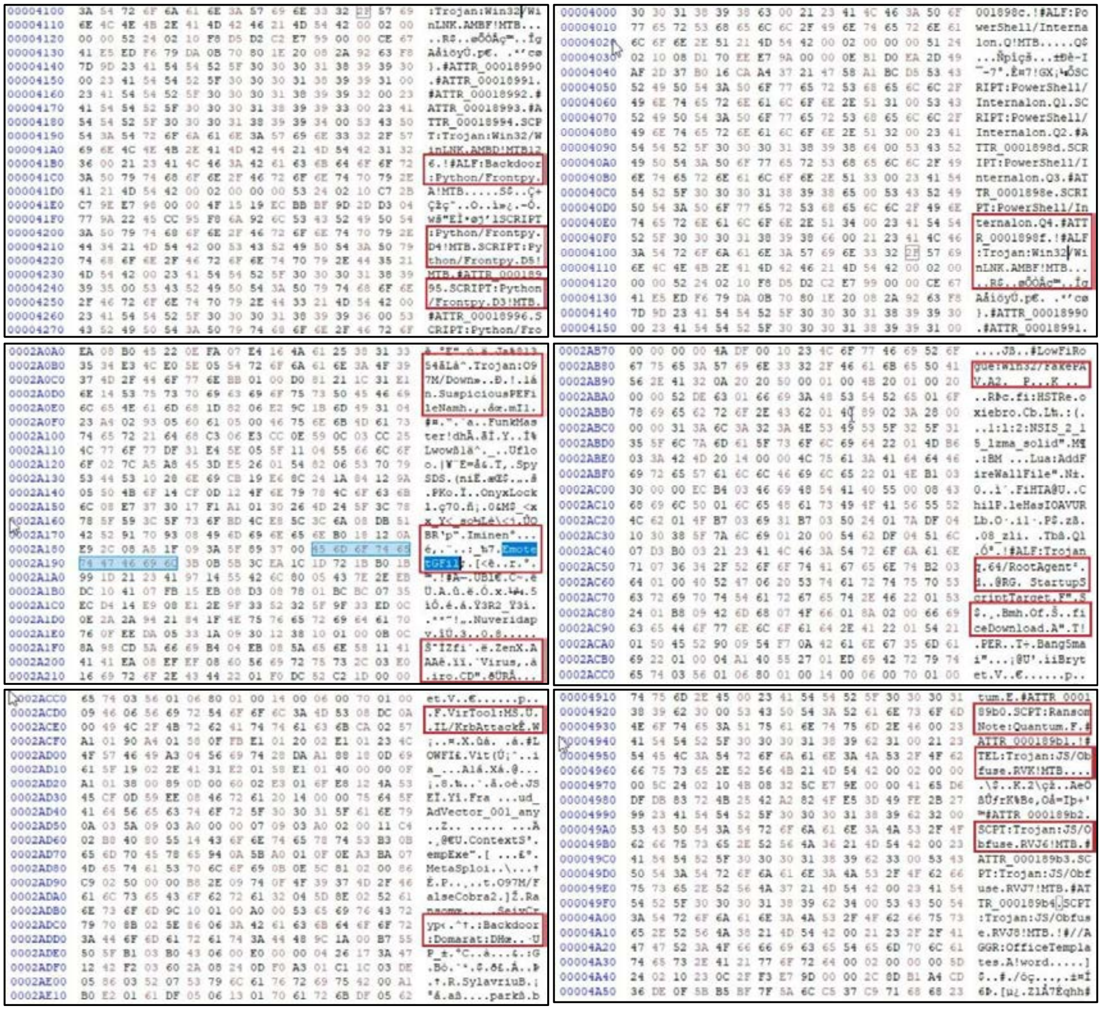


```
n=1310  kristiwayne92@gmail.com (utf16=491)
n=55    appro@openssl.org
n=35    sh0xzj+y2kbw714qyfw0yoid3zazk@guerrillamail.com (utf16=12)
n=15    pkiadmin@trustcentre.co.za
n=14    info@globaltrust.info
n=13    pki@sk.ee
n=11    info@e-szigno.hu
n=11    yne92@gmail.com (utf16=3)
n=9     sh0xzj@guerrillamail.com
n=8     microsoft365@notificationmail.microsoft.com     (utf16=3)
n=7     info@izenpe.com
n=6     googlecommunityteam-noreply@google.com
n=5     1796d24c4b2c353d6f35ef5382ef5980127@guerrillamail.com
n=5     57f7f8000f26e2c84a9cc068481b3efcb273@guerrillamail.com
n=5     ristiwayne92@gmail.com  (utf16=1)
n=4     admin_ca@mtin.es
n=4     chambersignroot@chambersign.org
n=4     chambersroot@chambersign.org
n=4     noreply@google.com
n=4     onedrive@notificationmail.microsoft.com
```

Figure 10: Email histogram

Findings: It depicts, there is a strong possibility that the host computer has been exposed/ open a backdoor by clicking any suspicious email/ attachments.

Analysis 4: We have analyzed all xml, html for malicious javascript embeddings. We use REMNUX tools to identify macros in excel and document files. We have also identified the presence of several Trojans, Spywares, Ransomwares, BOT in “wav”, “ttf” file. Figure 11 shows the possible exploitations.



```
00004100  3A 54 72 6F 6A 61 6E 3A 57 69 6E 33 32 2F 57 69  :Trojan:Win32/Wi
00004110  6E 4C 4E 4B 2E 41 4D 42 46 21 4D 54 42 00 02 00  nLNK.AMBF!MTB...
00004120  00 00 52 24 02 10 F8 D5 D2 C2 E7 99 00 00 CE 67  ..R$..øÕÒÂç™..Îg
00004130  41 E5 ED F6 79 DA 0B 70 80 1E 20 08 2A 92 63 F8  AåíöyÚ.p€. .*’cø
00004140  7D 9D 23 41 54 54 52 5F 30 30 30 31 38 39 39 30  }.#ATTR_00018990
00004150  00 23 41 54 54 52 5F 30 30 30 31 38 39 39 31 00  .#ATTR_00018991.
00004160  23 41 54 54 52 5F 30 30 30 31 38 39 39 32 00 23  #ATTR_00018992.#
00004170  41 54 54 52 5F 30 30 30 31 38 39 39 33 00 23 41  ATTR_00018993.#A
00004180  54 54 52 5F 30 30 30 31 38 39 39 34 00 53 43 50  TTR_00018994.SCP
00004190  54 3A 54 72 6F 6A 61 6E 3A 57 69 6E 33 32 2F 57  T:Trojan:Win32/W
000041A0  69 6E 4C 4E 4B 2E 41 4D 42 44 21 4D 54 42 31 32  inLNK.AMBD!MTB12
000041B0  36 00 21 23 41 4C 46 3A 42 61 63 6B 64 6F 6F 72  6.!#ALF:Backdoor
000041C0  3A 50 79 74 68 6F 6E 2F 46 72 6F 6E 74 70 79 2E  :Python/Frontpy.
000041D0  41 21 4D 54 42 00 02 00 00 00 53 24 02 10 C7 2B  A!MTB.....S$..Ç+
000041E0  C7 9E E7 98 00 00 4F 15 19 EC BB BF 9D 2D D3 04  Çžç˜..O..ì»¿.-Ó.
000041F0  77 9A 22 45 CC 95 F8 6A 92 6C 53 43 52 49 50 54  wš"EÌ•øj’lSCRIPT
00004200  3A 50 79 74 68 6F 6E 2F 46 72 6F 6E 74 70 79 2E  :Python/Frontpy.
00004210  44 34 21 4D 54 42 00 53 43 52 49 50 54 3A 50 79  D4!MTB.SCRIPT:Py
00004220  74 68 6F 6E 2F 46 72 6F 6E 74 70 79 2E 44 35 21  thon/Frontpy.D5!
00004230  4D 54 42 00 23 41 54 54 52 5F 30 30 30 31 38 39  MTB.#ATTR_000189
00004240  39 35 00 53 43 52 49 50 54 3A 50 79 74 68 6F 6E  95.SCRIPT:Python
00004250  2F 46 72 6F 6E 74 70 79 2E 44 33 21 4D 54 42 00  /Frontpy.D3!MTB.
00004260  23 41 54 54 52 5F 30 30 30 31 38 39 39 36 00 53  #ATTR_00018996.S
00004270  43 52 49 50 54 3A 50 79 74 68 6F 6E 2F 46 72 6F  CRIPT:Python/Fro
```

```
00004000  30 30 31 38 39 38 63 00 21 23 41 4C 46 3A 50 6F  001898c.!#ALF:Po
00004010  77 65 72 53 68 65 6C 6C 2F 49 6E 74 65 72 6E 61  werShell/Interna
00004020  6C 6F 6E 2E 51 21 4D 54 42 00 02 00 00 00 51 24  lon.Q!MTB.....Q$
00004030  02 10 08 D1 70 EE E7 9A 00 00 0E B1 D0 EA 2D 49  ...Ñpîçš...±Ðê-I
00004040  AF 2D 37 B0 16 CA A4 37 21 47 58 A1 BC D5 53 43  ¯-7°.Ê¤7!GX¡¼ÕSC
00004050  52 49 50 54 3A 50 6F 77 65 72 53 68 65 6C 6C 2F  RIPT:PowerShell/
00004060  49 6E 74 65 72 6E 61 6C 6F 6E 2E 51 31 00 53 43  Internalon.Q1.SC
00004070  52 49 50 54 3A 50 6F 77 65 72 53 68 65 6C 6C 2F  RIPT:PowerShell/
00004080  49 6E 74 65 72 6E 61 6C 6F 6E 2E 51 32 00 23 41  Internalon.Q2.#A
00004090  54 54 52 5F 30 30 30 31 38 39 38 64 00 53 43 52  TTR_0001898d.SCR
000040A0  49 50 54 3A 50 6F 77 65 72 53 68 65 6C 6C 2F 49  IPT:PowerShell/I
000040B0  6E 74 65 72 6E 61 6C 6F 6E 2E 51 33 00 23 41 54  nternalon.Q3.#AT
000040C0  54 52 5F 30 30 30 31 38 39 38 65 00 53 43 52 49  TR_0001898e.SCRI
000040D0  50 54 3A 50 6F 77 65 72 53 68 65 6C 6C 2F 49 6E  PT:PowerShell/In
000040E0  74 65 72 6E 61 6C 6F 6E 2E 51 34 00 23 41 54 54  ternalon.Q4.#ATT
000040F0  52 5F 30 30 30 31 38 39 38 66 00 21 23 41 4C 46  R_0001898f.!#ALF
00004100  3A 54 72 6F 6A 61 6E 3A 57 69 6E 33 32 2F 57 69  :Trojan:Win32/Wi
00004110  6E 4C 4E 4B 2E 41 4D 42 46 21 4D 54 42 00 02 00  nLNK.AMBF!MTB...
00004120  00 00 52 24 02 10 F8 D5 D2 C2 E7 99 00 00 CE 67  ..R$..øÕÒÂç™..Îg
00004130  41 E5 ED F6 79 DA 0B 70 80 1E 20 08 2A 92 63 F8  AåíöyÚ.p€. .*’cø
00004140  7D 9D 23 41 54 54 52 5F 30 30 30 31 38 39 39 30  }.#ATTR_00018990
00004150  00 23 41 54 54 52 5F 30 30 30 31 38 39 39 31 00  .#ATTR_00018991.
```

```
0002A0A0  EA 08 B0 45 22 0E FA 07 E4 16 4A 61 25 38 31 33  ê.°E".ú.ä.Ja%813
0002A0B0  35 34 E3 4C E0 5E 05 54 72 6F 6A 61 6E 3A 4F 39  54ãLà^.Trojan:O9
0002A0C0  37 4D 2F 44 6F 77 6E BB 01 00 D0 81 21 1C 31 E1  7M/Down»..Ð.!.1á
0002A0D0  6E 14 53 75 73 70 69 63 69 6F 75 73 50 45 46 69  n.SuspiciousPEFi
0002A0E0  6C 65 4E 61 6D 68 1D 82 06 E2 9C 1B 6D 49 31 04  leNamh.‚.âœ.mI1.
0002A0F0  23 A4 02 93 05 60 61 05 00 46 75 6E 6B 4D 61 73  #¤.".`a..FunkMas
0002A100  74 65 72 21 64 68 C3 06 E3 CC 0E 59 0C 03 CC 25  ter!dhÃ.ãÌ.Y..Ì%
0002A110  4C 77 6F 77 DF 31 E4 5E 05 5F 11 04 55 66 6C 6F  Lwowß1ä^._..Uflo
0002A120  6F 02 7C A5 A8 45 3D E5 26 01 54 82 06 53 70 79  o.|¥¨E=å&.T‚.Spy
0002A130  53 44 53 10 28 6E 69 CB 19 E6 8C 24 1A 84 12 9A  SDS.(niË.æŒ$.„.š
0002A140  05 50 4B 6F 14 CF 0D 12 4F 6E 79 78 4C 6F 63 6B  .PKo.Ï..OnyxLock
0002A150  6C 08 E7 37 30 17 F1 A1 01 30 26 4D 24 5F 3C 78  l.ç70.ñ¡.0&M$_<x
0002A160  78 5F 59 3C 5F 73 6F BD 4C E8 5C 3C 6A 08 DB 51  x_Y<_so½Lè\<j.ÛQ
0002A170  42 52 91 70 93 08 49 6D 69 6E 65 6E B0 18 12 0A  BR'p".Iminen°...
0002A180  E9 2C 08 A5 1F 09 3A 5F 89 37 00 45 6D 6F 74 65  é,.¥..:_‰7.Emote
0002A190  74 47 46 69 6C 3B 0B 5B 3C EA 1C 1D 72 1B B0 1B  tGFil;.[<ê..r.°.
0002A1A0  99 1D 21 23 41 97 14 55 42 6C 80 05 43 7E 2E EB  ™.!#A—.UBl€.C~.ë
0002A1B0  DC 10 41 07 FB 15 EB 08 D3 08 78 01 BC BC 07 35  Ü.A.û.ë.Ó.x.¼¼.5
0002A1C0  EC D4 14 E9 08 E1 2E 9F 33 52 32 5F 9F 33 ED 0C  ìÔ.é.á.Ÿ3R2_Ÿ3í.
0002A1D0  0E 2A 2A 94 21 84 1F 4E 75 76 65 72 69 64 61 70  .**"!„.Nuveridap
0002A1E0  76 0F EE DA 05 33 1A 09 30 12 38 10 01 00 0B 0C  v.îÚ.3..0.8.....
0002A1F0  8A 98 CD 5A 66 69 B4 04 EB 08 5A 65 6E 58 11 41  Š˜ÍZfi´.ë.ZenX.A
0002A200  41 41 EA 08 EF EF 08 60 56 69 72 75 73 2C 03 E0  AAê.ïï.`Virus,.à
0002A210  16 69 72 6F 2E 43 44 22 01 F0 DC 52 C2 1D 00 00  .iro.CD".ðÜRÂ...
```

```
0002AB70  00 00 00 00 4A DF 00 10 23 4C 6F 77 46 69 52 6F  ....Jß..#LowFiRo
0002AB80  67 75 65 3A 57 69 6E 33 32 2F 46 61 6B 65 50 41  gue:Win32/FakePA
0002AB90  56 2E 41 32 0A 20 20 50 00 01 00 4B 20 01 00 20  V.A2.  P...K .. 
0002ABA0  00 00 52 DE 63 01 66 69 3A 48 53 54 52 65 01 6F  ..RÞc.fi:HSTRe.o
0002ABB0  78 69 65 62 72 6F 2E 43 62 01 40 89 02 3A 28 00  xiebro.Cb.@‰.:(.
0002ABC0  00 00 31 3A 6C 3A 32 3A 4E 53 49 53 5F 32 5F 31  ..1:l:2:NSIS_2_1
0002ABD0  35 5F 6C 7A 6D 61 5F 73 6F 6C 69 64 22 01 4D B6  5_lzma_solid".M¶
0002ABE0  03 3A 42 4D 20 14 00 00 4C 75 61 3A 41 64 64 46  .:BM ...Lua:AddF
0002ABF0  69 72 65 57 61 6C 6C 46 69 6C 65 22 01 4E B1 03  ireWallFile".N±.
0002AC00  30 00 00 EC B4 03 46 69 48 54 41 40 55 00 08 43  0..ì´.FiHTA@U..C
0002AC10  68 69 6C 50 01 6C 65 48 61 73 49 4F 41 56 55 52  hilP.leHasIOAVUR
0002AC20  4C 62 01 4F B7 03 69 31 B7 03 50 24 01 7A DF 04  Lb.O·.i1·.P$.zß.
0002AC30  10 30 38 5F 7A 6C 69 01 20 00 54 62 DF 04 51 6C  .08_zli. .Tbß.Ql
0002AC40  07 D3 B0 03 21 23 41 4C 46 3A 54 72 6F 6A 61 6E  .Ó°.!#ALF:Trojan
0002AC50  71 07 36 34 2F 52 6F 6F 74 41 67 65 6E 74 B2 03  q.64/RootAgent².
0002AC60  64 01 00 40 52 47 06 20 53 74 61 72 74 75 70 53  d..@RG. StartupS
0002AC70  63 72 69 70 74 54 61 72 67 65 74 2E 46 22 01 53  criptTarget.F".S
0002AC80  24 01 B8 09 42 6D 68 07 4F 66 01 8A 02 00 66 69  $.¸.Bmh.Of.Š..fi
0002AC90  63 65 44 6F 77 6E 6C 6F 61 64 2E 41 22 01 54 21  ceDownload.A".T!
0002ACA0  01 50 45 52 90 09 54 F7 0A 42 61 6E 67 35 6D 61  .PER..T÷.Bang5ma
0002ACB0  69 22 01 00 04 A1 40 55 27 01 ED 69 42 72 79 74  i"...¡@U'.íiBryt
0002ACC0  65 74 03 56 01 06 80 01 00 14 00 06 00 70 01 00  et.V..€......p..
```

```
0002ACC0  65 74 03 56 01 06 80 01 00 14 00 06 00 70 01 00  et.V..€......p..
0002ACD0  09 46 06 56 69 72 54 6F 6F 6C 3A 4D 53 08 DC 0A  .F.VirTool:MS.Ü.
0002ACE0  00 49 4C 2F 4B 72 62 41 74 74 61 63 6B CA 02 57  .IL/KrbAttackÊ.W
0002ACF0  A1 01 90 A4 01 58 0F FB E1 01 20 02 E1 01 23 4C  ¡..¤.X.ûá. .á.#L
0002AD00  4F 57 46 49 A3 04 56 69 74 28 DA A1 88 18 0D 69  OWFI£.Vit(Ú¡ˆ..i
0002AD10  61 5F 19 02 2E 41 31 E2 01 58 E1 01 40 00 00 0F  a_...A1â.Xá.@...
0002AD20  A1 01 38 00 89 0D 00 60 02 E3 01 6F E8 12 4A 53  ¡.8.‰..`.ã.oè.JS
0002AD30  45 CF 0D 59 EE 08 46 72 61 20 14 00 00 75 64 5F  EÏ.Yî.Fra ...ud_
0002AD40  41 64 56 65 63 74 6F 72 5F 30 30 31 5F 61 6E 79  AdVector_001_any
0002AD50  0A 03 5A 09 03 A0 00 00 07 09 03 A0 02 00 11 C4  ..Z.. ..... ...Ä
0002AD60  02 B8 40 80 55 14 43 6F 6E 74 65 78 74 53 B3 0B  .¸@€U.ContextS³.
0002AD70  65 6D 70 45 78 65 94 0A 5B A0 01 0F 0E A3 BA 07  empExe".[ ...£º.
0002AD80  4D 65 74 61 53 70 6C 6F 69 0B 0E 5C 81 02 00 86  MetaSploi..\...†
0002AD90  C9 02 50 00 00 B8 2E 09 74 0F 4F 39 37 4D 2F 46  É.P..¸..t.O97M/F
0002ADA0  61 6C 73 65 43 6F 62 72 61 32 04 5D 8E 02 52 61  alseCobra2.]Ž.Ra
0002ADB0  6E 73 6F 6D 9C 10 01 00 A0 00 53 65 69 76 43 72  nsomœ... .SeivCr
0002ADC0  79 70 8B 02 5E 86 06 3A 42 61 63 6B 64 6F 6F 72  yp‹.^†.:Backdoor
0002ADD0  3A 44 6F 6D 61 72 61 74 3A 44 48 9C 1A 00 B7 55  :Domarat:DHœ..·U
0002ADE0  50 5F B1 03 B0 43 06 00 E0 00 00 04 26 17 3A 47  P_±.°C..à...&.:G
0002ADF0  12 42 F2 03 60 2A 08 24 0D F0 A3 01 C1 1C 03 DE  .Bò.`*.$.ð£.Á..Þ
0002AE00  05 86 03 52 07 53 79 6C 61 76 72 69 75 42 00 A1  .†.R.SylavriuB.¡
0002AE10  B0 E2 01 61 DF 05 06 13 01 70 61 72 6B DF 05 62  °â.aß....parkß.b
```

```
00004910  74 75 6D 2E 45 00 23 41 54 54 52 5F 30 30 30 31  tum.E.#ATTR_0001
00004920  38 39 62 30 00 53 43 50 54 3A 52 61 6E 73 6F 6D  89b0.SCPT:Ransom
00004930  4E 6F 74 65 3A 51 75 61 6E 74 75 6D 2E 46 00 23  Note:Quantum.F.#
00004940  41 54 54 52 5F 30 30 30 31 38 39 62 31 00 21 23  ATTR_000189b1.!#
00004950  54 45 4C 3A 54 72 6F 6A 61 6E 3A 4A 53 2F 4F 62  TEL:Trojan:JS/Ob
00004960  66 75 73 65 2E 52 56 4B 21 4D 54 42 00 02 00 00  fuse.RVK!MTB....
00004970  00 5C 24 02 10 4B 08 32 5C E7 9E 00 00 41 65 D6  .\$..K.2\çž..AeÖ
00004980  DF DB 83 72 4B 25 42 A2 82 4F E5 3D 49 FE 2B 27  ßÛƒrK%B¢‚Oå=Iþ+'
00004990  99 23 41 54 54 52 5F 30 30 30 31 38 39 62 32 00  ™#ATTR_000189b2.
000049A0  53 43 50 54 3A 54 72 6F 6A 61 6E 3A 4A 53 2F 4F  SCPT:Trojan:JS/O
000049B0  62 66 75 73 65 2E 52 56 4A 36 21 4D 54 42 00 23  bfuse.RVJ6!MTB.#
000049C0  41 54 54 52 5F 30 30 30 31 38 39 62 33 00 53 43  ATTR_000189b3.SC
000049D0  50 54 3A 54 72 6F 6A 61 6E 3A 4A 53 2F 4F 62 66  PT:Trojan:JS/Obf
000049E0  75 73 65 2E 52 56 4A 37 21 4D 54 42 00 23 41 54  use.RVJ7!MTB.#AT
000049F0  54 52 5F 30 30 30 31 38 39 62 34 00 53 43 50 54  TR_000189b4.SCPT
00004A00  3A 54 72 6F 6A 61 6E 3A 4A 53 2F 4F 62 66 75 73  :Trojan:JS/Obfus
00004A10  65 2E 52 56 4A 38 21 4D 54 42 00 21 23 2F 2F 41  e.RVJ8!MTB.!#//A
00004A20  47 47 52 3A 4F 66 66 69 63 65 54 65 6D 70 6C 61  GGR:OfficeTempla
00004A30  74 65 73 2E 41 21 77 6F 72 64 00 02 00 00 00 5D  tes.A!word.....]
00004A40  24 02 10 23 0C 2F F3 E7 9D 00 00 2C 8D B1 A4 CD  $..#./óç...,.±¤Í
00004A50  36 DE 0F 5B B5 BF 7F 5A 6C C5 37 C9 71 68 68 23  6Þ.[µ¿.ZlÅ7Éqhh#
```

Figure 11: Exploitation evidence in “wav”, “ttf” files

Findings: The “Zero Event” is unidentifiable.

Analysis 5: We have used “Bulk Extractor” to analyze the dump file further. “Bulk Extractor” usually extract data from the source sequentially. Therefore, we may presume that the extracted data are in the format that is consecutive and timely. The findings are listed in table 2.

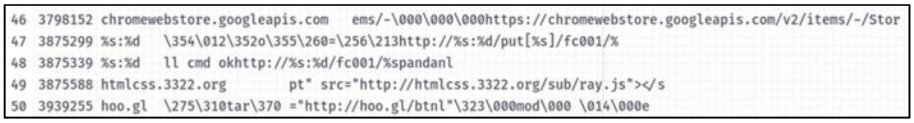
Criteria	Information based on Criteria	# of items
url	10 MB	
domain	4.3 MB	
json	3.2 MB	
rfc	57.2 KB	
pcap	52.9 KB	
url_service	207.6 KB	
AES128 key	5.1 KB	48
AES256 key	4.1 KB	30

RSA key	154.6	49

Table 2: Volume of information extracted by Bulk Extractor

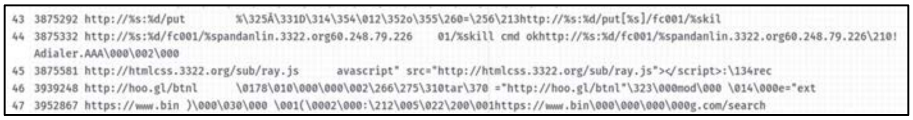
Findings:

1) Based on the “url”, “url_service”, “domain surf”, and “json” dump, it is evident that the browsed URLs are as illustrated in figure 12(a)(b)(c)(d).



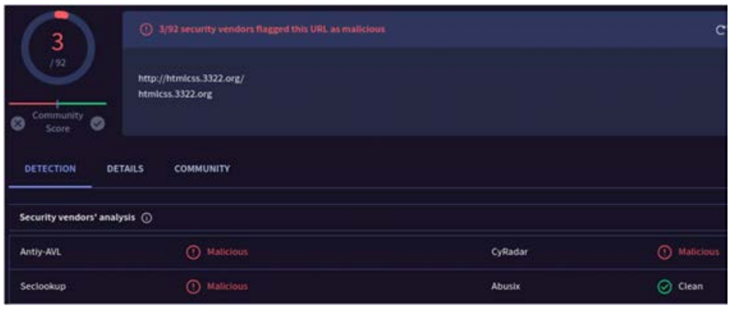
```
46 3798152 chromewebstore.googleapis.com   ems/-\000\000\000https://chromewebstore.googleapis.com/v2/items/-/Stor
47 3875299 %s:%d   \354\012\352o\355\260=\256\213http://%s:%d/put[%s]/fc001/%
48 3875339 %s:%d   ll cmd okhttp://%s:%d/fc001/%spandanl
49 3875588 htmlcss.3322.org        pt" src="http://htmlcss.3322.org/sub/ray.js"></s
50 3939255 hoo.gl  \275\310tar\370 ="http://hoo.gl/btnl"\323\000mod\000 \014\000e
```

Figure 12(a): URL timeline



```
43 3875292 http://%s:%d/put        %\325Ã\331D\314\354\012\352o\355\260=\256\213http://%s:%d/put[%s]/fc001/%skil
44 3875332 http://%s:%d/fc001/%spandanlin.3322.org60.248.79.226    01/%skill cmd okhttp://%s:%d/fc001/%spandanlin.3322.org60.248.79.226\210!
   Adialer.AAA\000\002\000
45 3875581 http://htmlcss.3322.org/sub/ray.js      avascript" src="http://htmlcss.3322.org/sub/ray.js"></script>:\134rec
46 3939248 http://hoo.gl/btnl      \0178\010\000\000\002\266\275\310tar\370 ="http://hoo.gl/btnl"\323\000mod\000 \014\000e="ext
47 3952867 https://www.bin )\000\030\000 \001(\0002\000:\212\005\022\200\001https://www.bin\000\000\000\000g.com/search
```

Figure 12(b): URL Service timeline



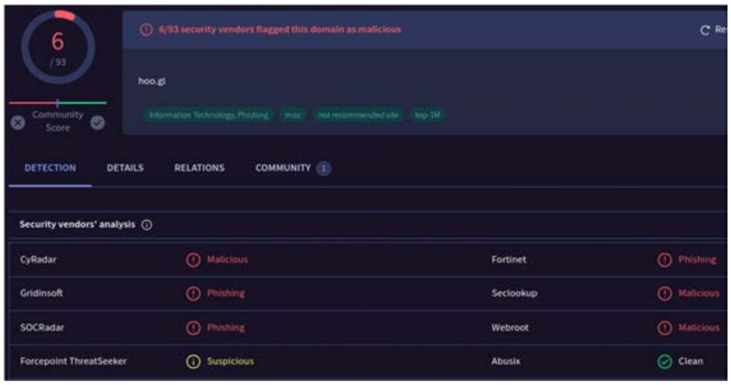
3/92 security vendors flagged this URL as malicious

http://htmlcss.3322.org/
htmlcss.3322.org

Security vendors' analysis

Antiy-AVL	Malicious	CyRadar	Malicious
Seclookup	Malicious	Abusix	Clean

Figure 12(c): “Virus Total” response for “http://htmlcss.3322.org”



6/93 security vendors flagged this domain as malicious

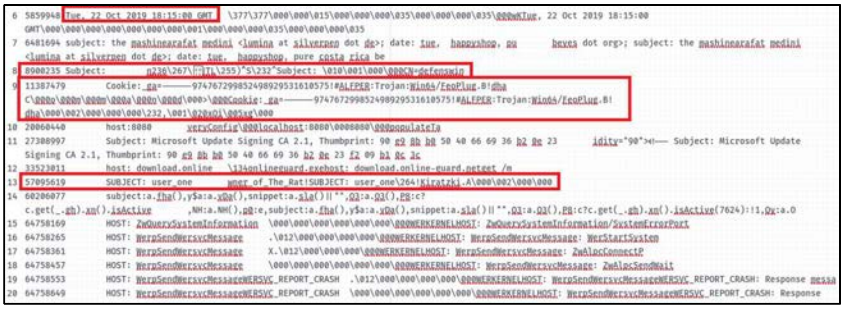
hoo.gl

Security vendors' analysis

CyRadar	Malicious	Fortinet	Phishing
Gridinsoft	Phishing	Seclookup	Malicious
SOCRadar	Phishing	Webroot	Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean

Figure 12(d): “Virus Total” response for “http://hoo.gl”

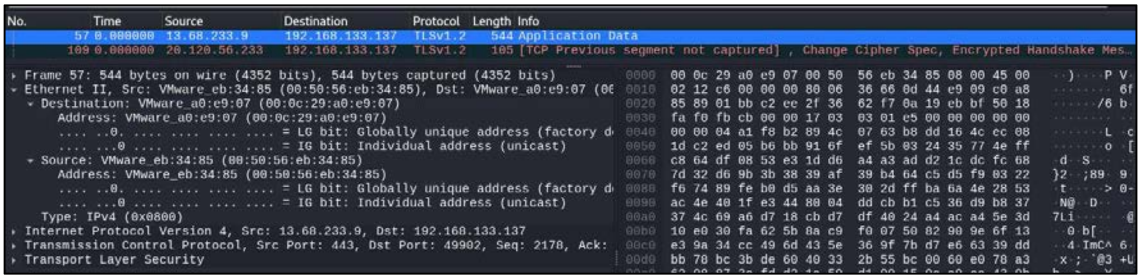
2) The “rfc822” extraction informs that a “cookie” file has been fetched which contained backdoor application.



```
6  5859948 Tue, 22 Oct 2019 18:15:00 GMT   \377\377\000\000\015\000\000\000\035\000\000\000\035\000wKTue, 22 Oct 2019 18:15:00
   GMT\000\000\000\000\000\000\000\001\000\000\000\035\000\000\000\035
7  6481694 subject: the mashinearafat medini <lumina at silverpen dot de>; date: tue,  happyshop, pu      beyes dot org>; subject: the mashinearafat medini
   <lumina at silverpen dot de>; date: tue,  happyshop, pure costa rica be
8  8900235 Subject:         n236\267\□ITL\255)^S\232^Subject: \010\001\000\000CN=defenswin
9  11387479         Cookie: _ga=———974767299852498929531610575!#ALFPER:Trojan:Win64/FeoPlug.B!dha
   C\000o\000n\000m\000a\000n\000d\000>\000Cookie: _ga=———974767299852498929531610575!#ALFPER:Trojan:Win64/FeoPlug.B!
   dha\000\002\000\000\000\232,\001\020xOi\005xg\000
10 20060440         host:8080       veryConfig\000localhost:8080\0008080\000populateIa
11 27308997         Subject: Microsoft Update Signing CA 2.1, Thumbprint: 90 e9 8b b0 50 40 66 69 36 b2 0e 23       idity="90">ⅎ—— Subject: Microsoft Update
   Signing CA 2.1, Thumbprint: 90 e9 8b b0 50 40 66 69 36 b2 0e 23 f2 09 b1 0c 3c
12 33523011         host: download.online   \134onlineguard.exehost: download.online-guard.netget /m
13 57095619         SUBJECT: user_one       wner_of_The_Rat!SUBJECT: user_one\264!Kiratzki.A\000\002\000\000
14 60206077         subject:a.fha(),y$a:a.yDa(),snippet:a.sla()||"",O3:a.O3(),P8:c?
   c.get(_.gh).xn().isActive       ,NH:a.NH(),p0:e,subject:a.fha(),y$a:a.yDa(),snippet:a.sla()||"",O3:a.O3(),P8:c?c.get(_.gh).xn().isActive(7624):!1,Qy:a.O
15 64758169         HOST: ZwQuerySystemInformation  \000\000\000\000\000\000\000WERKERNELHOST: ZwQuerySystemInformation/SystemErrorPort
16 64758265         HOST: WerpSendWersvcMessage     .\012\000\000\000\000\000WERKERNELHOST: WerpSendWersvcMessage: WerStartSysten
17 64758361         HOST: WerpSendWersvcMessage     X.\012\000\000\000\000WERKERNELHOST: WerpSendWersvcMessage: ZwAlpcConnectP
18 64758457         HOST: WerpSendWersvcMessage     \000\000\000\000\000\000\000WERKERNELHOST: WerpSendWersvcMessage: ZwAlpcSendWait
19 64758553         HOST: WerpSendWersvcMessageWERSVC_REPORT_CRASH  .\012\000\000\000\000\000WERKERNELHOST: WerpSendWersvcMessageWERSVC_REPORT_CRASH: Response messa
20 64758649         HOST: WerpSendWersvcMessageWERSVC_REPORT_CRASH  \000\000\000\000\000\000\000WERKERNELHOST: WerpSendWersvcMessageWERSVC_REPORT_CRASH: Response
```

Figure 13: Pre-fetched Cookie

3) A “pecap” file has been extracted with 254 packets. We have examined this “pacap” files and confirmed the foreign IPs 13.68.233.9 and 20.120.56.233 share the same “mac” address. Also, there are 2 TLS packets with encrypted data as shown in figure 14.



```
No.    Time      Source          Destination      Protocol  Length Info
    57 0.000000  13.68.233.9     192.168.133.137  TLSv1.2    544 Application Data
   109 0.000000  20.120.56.233   192.168.133.137  TLSv1.2    105 [TCP Previous segment not captured] , Change Cipher Spec, Encrypted Handshake Mes…

▸ Frame 57: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits)            0000  00 0c 29 a0 e9 07 00 50  56 eb 34 85 08 00 45 00   ··)····P V·
▾ Ethernet II, Src: VMware_eb:34:85 (00:50:56:eb:34:85), Dst: VMware_a0:e9:07 (0€    0010  02 12 c6 00 00 00 80 06  36 66 0d 44 e9 09 c0 a8   ········ 6f
  ▾ Destination: VMware_a0:e9:07 (00:0c:29:a0:e9:07)                                 0020  85 89 01 bb c2 ee 2f 36  62 f7 0a 19 eb bf 50 18   ······/6 b·
      Address: VMware_a0:e9:07 (00:0c:29:a0:e9:07)                                   0030  fa f0 fb cb 00 00 17 03  03 01 e5 00 00 00 00 00   ·········
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory d     0040  00 00 04 a1 f8 b2 89 4c  07 63 b8 dd 16 4c ec 08   ·······L ·c
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)          0050  1d c2 ed 05 b6 bb 91 6f  ef 5b 03 24 35 77 4e ff   ·······o ·[
  ▾ Source: VMware_eb:34:85 (00:50:56:eb:34:85)                                      0060  c8 64 df 08 53 e3 1d d6  a4 a3 ad d2 1c dc fc 68   ·d··S···
      Address: VMware_eb:34:85 (00:50:56:eb:34:85)                                   0070  7d 32 d6 9b 3b 38 39 af  39 b4 64 c5 d5 f9 03 22   }2··;89· 9
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory d     0080  f6 74 89 fe b0 d5 aa 3e  30 2d ff ba 6a 4e 28 53   ·t·····> 0-
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)          0090  ac 4e 40 1f e3 44 80 04  dd cb b1 c5 36 d9 b8 37   ·N@··D··
    Type: IPv4 (0x0800)                                                              00a0  37 4c 69 a6 d7 18 cb d7  df 40 24 a4 ac a4 5e 3d   7Li·····  ·@
▸ Internet Protocol Version 4, Src: 13.68.233.9, Dst: 192.168.133.137                00b0  10 e0 30 fa 62 5b 8a c9  f0 07 50 82 90 9e 6f 13   ··0·b[··
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 49902, Seq: 2178, Ack:     00c0  e3 9a 34 cc 49 6d 43 5e  36 9f 7b d7 e6 63 39 dd   ··4·ImC^ 6·
▸ Transport Layer Security                                                           00d0  bb 78 bc 3b de 60 40 33  2b 55 bc 00 60 e0 78 a3   ·x·;·`@3 +U
```

Figure 14: 2 TLS Packets with encrypted payload

We have made an effort to decode the payload using 49 retrieved RSA keys. There are two private keys and 47 public keys among them. The keys are in DER format. we are unable to convert the RSA keys to PEM or Base64 format since they are all corrupted.

3.3 (A4) Network traffic log analysis

Software used: Wireshark, NetworkMiner, DrawIO

There are 208335 packets in the Network log. To find the appropriate “Source” for the destination “192.168.10.45”, we develop a traceback program (written in Python v 3.12). Here we use “Depth First Search (DFS)” algorithm to traceback the source that transferred packets to the PLC module. The figure 15(a)(b)(c) shows the responsible “source(s)” for the exploitations.

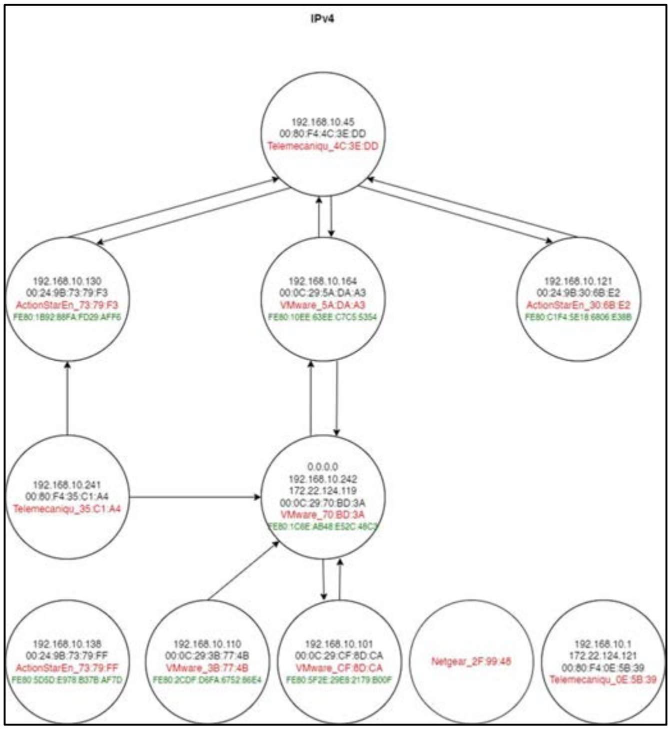


Figure 15(a): Packet transfer to 192.168.10.45 (ipv4)

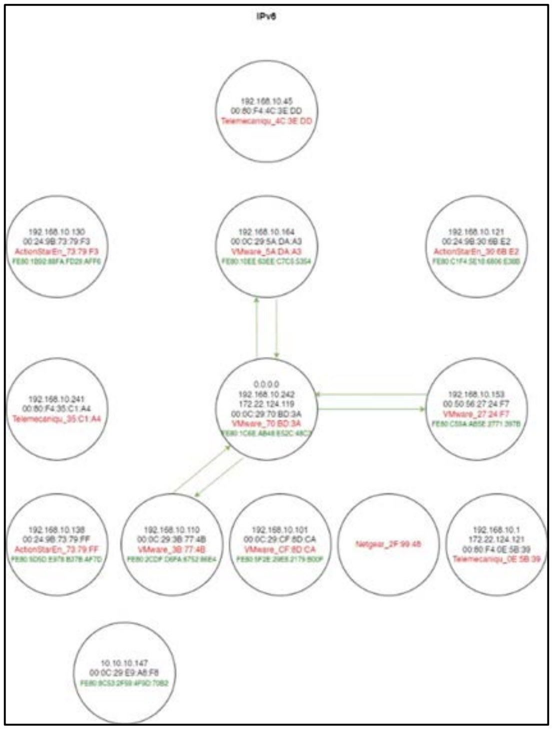


Figure 15(b): Packet transfer to 192.168.10.45 (ipv6)

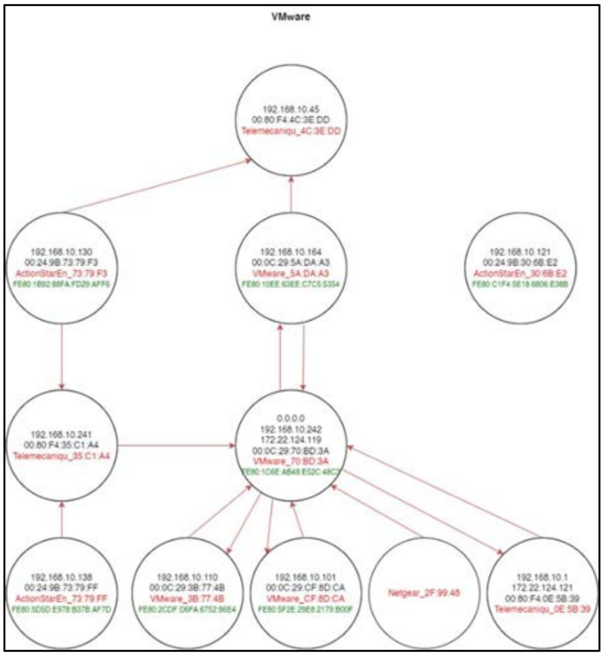
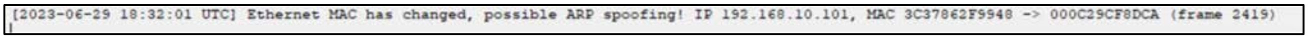


Figure 15(c): Packet transfer to 192.168.10.45 (VM)

A possible alteration of mac address has been observed at frame 2419 as show in the figure 16.



```
[2023-06-29 18:32:01 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.101, MAC 3C37862F9948 -> 000C29CF8DCA (frame 2419)
```

Figure 16: ARP spoofing

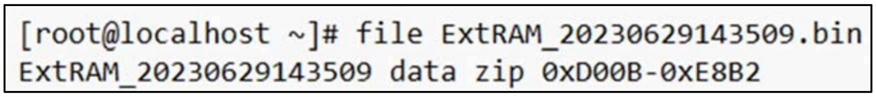
Findings: We found 3 workstations bearing IP 192.168.10.121, 192.168.10.130, and 192.168.10.164 transferred packets directly to 192.168.10.45.

3.4 (A5) External PLC Memory dumps analysis

Software used: Wireshark, Network Miner, HxD, Bless, “binwalk” (Kali Linux)

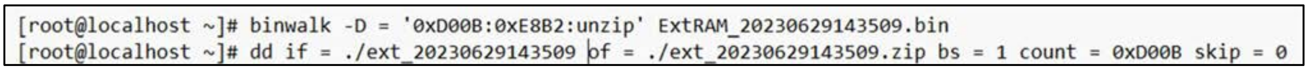
There are 7 external PLC memory dumps in binary. Each file has been named with the format “YYYYMMDDHMS” (ex. ExtRAM_20230629143509.bin), which denotes the time of memory acquisition.

Engineers can review the system's states with the assistance of the external memory unit, which periodically performs backups of the system. No data is taken from external memory by the PLC. The following command mentioned in figure 17 has been used to extract the metadata of a file. This Metadata shows if there exists any encapsulated data with the offset address or not. We have used “binwalk” to extract data also known as “file curving”, defined in figure 18.



```
[root@localhost ~]# file ExtRAM_20230629143509.bin
ExtRAM_20230629143509 data zip 0xD00B-0xE8B2
```

Figure 17: Bulk Extractor (Kali Linux) command to investigate these binary files



```
[root@localhost ~]# binwalk -D = '0xD00B:0xE8B2:unzip' ExtRAM_20230629143509.bin
[root@localhost ~]# dd if = ./ext_20230629143509 of = ./ext_20230629143509.zip bs = 1 count = 0xD00B skip = 0
```

Figure 18: File curving

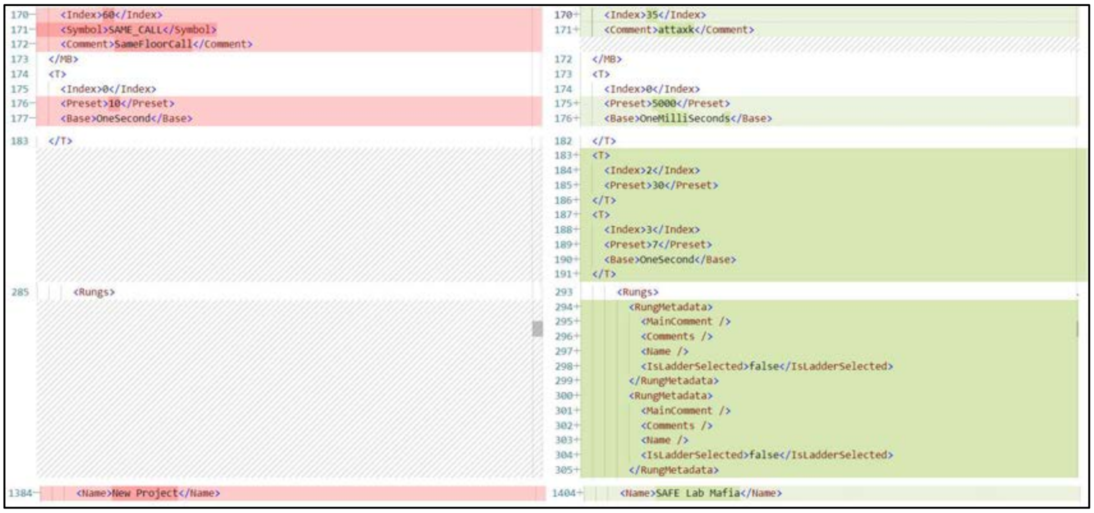
Seven XML files that show the PLC's current status were recovered from each memory dump. We measure the differences between each XML and the following XML. Table 3 shows the number of differences among the consecutive XMLs, whereas the figure 19(a)(b)(c) demonstrate the examples of the differences.

Label	XML (x)	XML (y)	Number of differences
ExpA_B	(ExtA) ext_20230629143509	(ExtB) ext_20230629145014	-
ExpA_C	(ExtA) ext_20230629143509	(ExtC) ext_20230629150519	5
ExpA_D	(ExtA) ext_20230629143509	(ExtD) ext_20230629152024	5
ExpC_D	(ExtC) ext_20230629150519	(ExtD) ext_20230629152024	-
ExpA_E	(ExtA) ext_20230629143509	(ExtE) ext_20230629153528	4
ExpC_E	(ExtC) ext_20230629150519	(ExtE) ext_20230629153528	4
ExpA_F	(ExtA) ext_20230629143509	(ExtF) ext_20230629155033	1
ExpC_F	(ExtC) ext_20230629150519	(ExtF) ext_20230629155033	4
ExpE_F	(ExtE) ext_20230629153528	(ExtF) ext_20230629155033	3
ExpE_G	(ExtE) ext_20230629153528	(ExtG) ext_20230629160538	3
ExpA_G	(ExtA) ext_20230629143509	(ExtG) ext_20230629160538	1

ExpC_G	(ExtC) ext_20230629150519	(ExtG) ext_20230629160538	4
ExpF_G	(ExtF) ext_20230629155033	(ExtG) ext_20230629160538	-

Table 3: Difference between 2 extracted XMLs from External PLC Memory

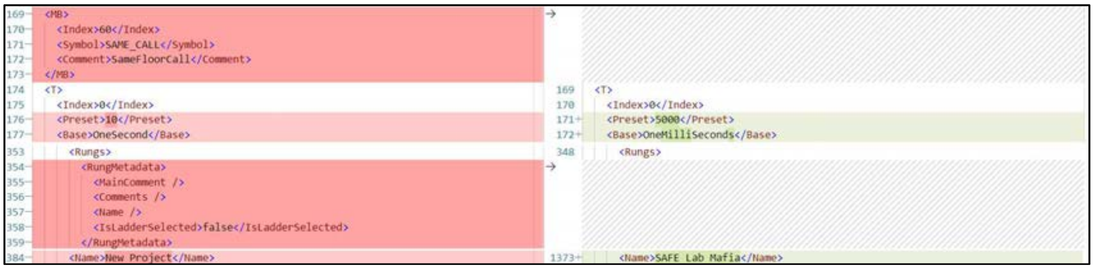
So, the XML changes timeline is: (ExtA, ExtB) → (ExtC, ExtD) → ExtE → ExtF → ExtG. Additionally, it indicates the PLC "attack" time: (ExtA, ExtB) → (ExtC, ExtD), that is the transition time between ExtB to ExtC, 14:50:14 to 15:05:19.



```
-    <Index>60</Index>
-    <Symbol>SAME_CALL</Symbol>
-    <Comment>SameFloorCall</Comment>
  </MB>
  <T>
    <Index>0</Index>
-    <Preset>10</Preset>
-    <Base>OneSecond</Base>
  </T>
      <Rungs>
-      <Name>New Project</Name>
```

```
+    <Index>35</Index>
+    <Comment>attaxk</Comment>
  </MB>
  <T>
    <Index>0</Index>
+    <Preset>5000</Preset>
+    <Base>OneMilliSeconds</Base>
  </T>
+  <T>
+    <Index>2</Index>
+    <Preset>30</Preset>
+  </T>
+  <T>
+    <Index>3</Index>
+    <Preset>7</Preset>
+    <Base>OneSecond</Base>
+  </T>
      <Rungs>
+        <RungMetadata>
+          <MainComment />
+          <Comments />
+          <Name />
+          <IsLadderSelected>false</IsLadderSelected>
+        </RungMetadata>
+        <RungMetadata>
+          <MainComment />
+          <Comments />
+          <Name />
+          <IsLadderSelected>false</IsLadderSelected>
+        </RungMetadata>
+      <Name>SAFE Lab Mafia</Name>
```

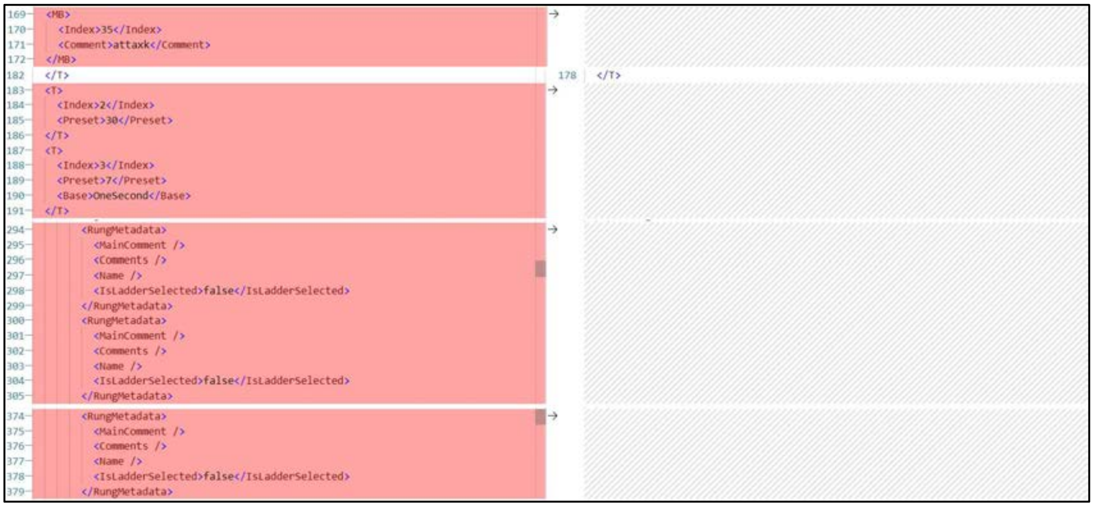
Figure 19(a): XML Differences of ExpA_C



```
-  <MB>
-    <Index>60</Index>
-    <Symbol>SAME_CALL</Symbol>
-    <Comment>SameFloorCall</Comment>
-  </MB>
  <T>
    <Index>0</Index>
-    <Preset>10</Preset>
-    <Base>OneSecond</Base>
      <Rungs>
-        <RungMetadata>
-          <MainComment />
-          <Comments />
-          <Name />
-          <IsLadderSelected>false</IsLadderSelected>
-        </RungMetadata>
-      <Name>New Project</Name>
```

```
  <T>
    <Index>0</Index>
+    <Preset>5000</Preset>
+    <Base>OneMilliSeconds</Base>
      <Rungs>
+      <Name>SAFE Lab Mafia</Name>
```

Figure 19(b): XML Difference of ExpA_E



```
<MB>
  <Index>35</Index>
  <Comment>attaxk</Comment>
</MB>
</T>
<T>
  <Index>2</Index>
  <Preset>30</Preset>
</T>
<T>
  <Index>3</Index>
  <Preset>7</Preset>
  <Base>OneSecond</Base>
</T>
      <RungMetadata>
        <MainComment />
        <Comments />
        <Name />
        <IsLadderSelected>false</IsLadderSelected>
      </RungMetadata>
      <RungMetadata>
        <MainComment />
        <Comments />
        <Name />
        <IsLadderSelected>false</IsLadderSelected>
      </RungMetadata>
      <RungMetadata>
        <MainComment />
        <Comments />
        <Name />
        <IsLadderSelected>false</IsLadderSelected>
      </RungMetadata>
```

```
</T>
```

Figure 19(c): XML Difference of ExpC_E

Findings: The external memory analysis proves the change in On-Chip PLC memory happens between 14:50:14 to 15:05:19.

3.5 (A6) On-Chip PLC Memory dumps analysis

Software used: Bulk Extractor (Kali Linux), HxD, Bless, Wireshark, Network Miner

Theory:

After carefully reviewing the provided artifact (A4) Network Traffic Logs (pcapng), we were able to identify the workstations (IP 192.168.10.121, 192.168.10.130, 192.168.10.164) that were in charge of sending packets to the PLC (IP 198.168.10.45). Additionally, we discovered that throughout those entire sessions, the Modbus TCP protocol was utilized.

Modbus TCP Protocol Specification:

The typical Modbus TCP protocol header, "Function Codes", "UMAS Codes", "Response Codes" and "Exceptions" are given in table 4, 5, 6, and 7.

Transection Identifier	**Protocol Identifier**	**Length Field**	**Unit ID**	**PDU**			
				Function Code	**Session ID**	**Data**	
						UMAS Code	**Data**
2 B	2 B	2 B	1 B	1 B	1 B	1 B	Variable

Table 4: Modbus TCP Specification

Function Code		Description
Hex	Decimal	
0x01	1	Read Coil Status
0x02	2	Read Input Status (Discrete)
0x03	3	Read Multiple Holding Registers
0x04	4	Read Input Registers
0x05	5	Force Write Single Coil
0x06	6	Force Write Single Holding Register
0x07	7	Read Exception Status
0x08	8	Diagnostic
	Sub-function Code	
	00	“echo mode" (Return Query Data)
	01	Restart Communication Option
	02	Return Diagnostic Register
	03	Change ASCII Input Delimiter
	04	Force Listen Only Mode
	10	Clear Counters and Diagnostic Register
	11	"counter 1" (Return Bus Message Count)
	12	"counter 2" (Return Bus Communication Error Count)
	13	"counter 3" (Return Bus Exception Error Count)
	16	"counter 6" (Return Slave NAK Count)
	17	"counter 7" (Return Slave Busy Count)
	18	"counter 8" (Return Bus Character Overrun Count)
0x0B	11	Get COM Event Counter
0x0C	12	Get COM Event Log
0x0F	15	Force Write Multiple Coils
0x10	16	Preset Multiple Registers/ Write Multiple Holding Registers
0x11	17	Report Slave ID
0x14	20	Read File Record
0x15	21	Write File Record
0x16	22	Mask Write Register
0x17	23	Read/ Write Multiple Registers
0x18	24	Read FIFO Queue
0x28	43	Read Device Identification/ Encapsulated Interface Transport
0x5A	90	Request/ Reply Packet

Table 5: Function codes of Modbus TCP

UMAS Code		Description
Hex	Decimal	
0x01	1	INIT_COMM: Initialize a UMAS communication
0x02	2	READ_ID: Read a PLC ID
0x03	3	READ_PROJECT_INFO
0x04	4	READ_PLC_INFO: Get internal PLC info
0x06	6	READ_CARD_INFO: Get internal PLC SD-Card info

0x0A	10	REPEAT: Data sent back to PLC
0x10	16	TAKE_PLC_RESERVATION: Assign an “owner” to the PLC
0x11	17	RELEASE_PLC_RESERVATION
0x12	18	KEEP_ALIVE: Keep alive message
0x20	32	READ_MEMORY_BLOCK
0x21	33	WRITE_MEMORY_BLOCK
0x22	34	READ_VARIABLES
0x23	35	WRITE_VARIABLS
0x24	36	READ_COILS_REGISTERS
0x25	37	WRITE_COILS_REGISTERS
0x28	40	READ_FNC
0x29	41	WRITE_FNC
0x30	48	INITIALIZE_UPLOAD: HMI to PLC
0x31	49	UPLOAD_BLOCK: HMI to PLC
0x32	50	END_STRATEGY_UPLOAD: HMI to PLC
0x33	51	INITIALIZE_UPLOAD: PLC to HMI
0x34	52	DOWNLOAD_BLOCK: PLC to HMI
0x35	53	END_STRATEGY_UPLOAD: PLC to HMI
0x39	57	READ_ETH_MASTER_DATA
0x40	64	START_PLC
0x41	65	STOP_PLC
0x50	80	MONITOR_PLC
0x58	88	CHECK_PLC
0x6D	109	COM_ERROR: Service Discontinued
0x70	112	READ_IO_OBJECT
0x71	113	WRITE_IO_OBJECT
0x73	115	GET_STATUS_MODULE

Table 6: UMAS Codes for Modbus TCP

Response Code		**Description**
Hex	**Decimal**	
0xFD	253	ERROR
0xFE	254	OK

Table 7: Modbus Response Codes

Analysis 1:

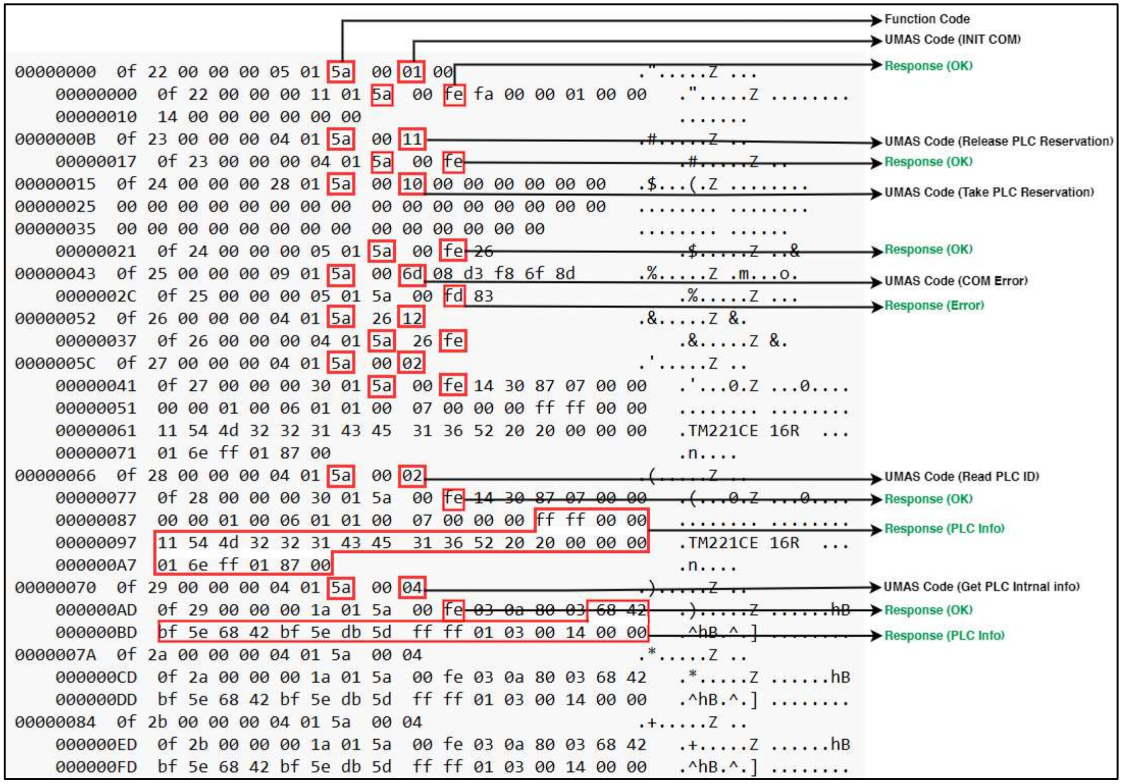
We have reexamined the (A4) Network Log Files artifact and decoded all the Modbus TCP transmissions. Our primary objective in this analysis is to identify the “Write” instructions (UMAS Code: 0x23 and 0x29) only for the PLC system (IP 192.168.10.45). We have isolated following frames form the given Network Log files for this investigation in table 8:

Source IP	**Number of Frames**	**Session**	**Frame Range**	**UMAS Code (0x23: Write_Variables or 0x29: Write_FNC)**
192.168.10.164	1755	1	50 – 1730	186 – 302

	130	2	1751 – 1882	–
	1777	3	46835 – 47318	47116 – 47234
	253	4	47603 – 47997	–
	489	5	85942 – 86814	86200 – 86314
	499	6	115698 – 116617	115961 – 116096
192.168.10.130	16	1	1 – 17	–
	4454	2	5465 – 11130	–
	1122	3	28896 - 30017	–
	4454	4	30085 – 34610	–
	1122	5	52660 – 53851	–
	4454	6	53918 – 58474	–
	1122	7	75057 – 76179	–
	4454	8	76335 – 80877	–
	1122	9	97432 – 98569	–
	4454	10	98798 – 103319	–
	1122	11	119874 – 120997	–
	4454	12	121291 – 125835	–
	30873	13	131815 – 208335	–
192.168.10.121	67681	–	2167 – 208330	–

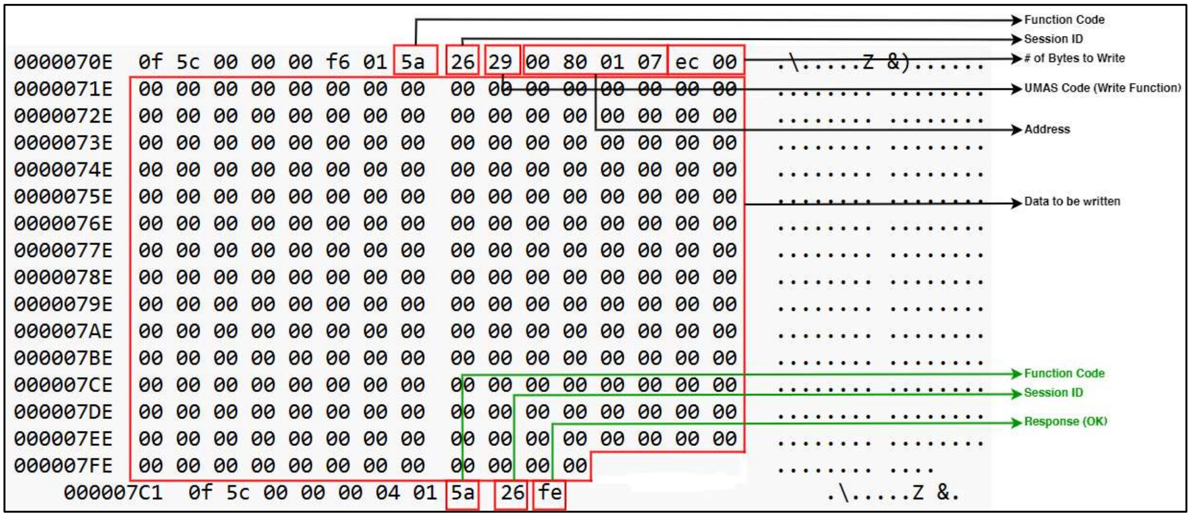
Table 8: Inspection of "Write" UMAS instruction for PLC System

Figure 20 and 21 show the decoded Modbus TCP transmissions using UMAS encoding.



```
00000000  0f 22 00 00 00 05 01 5a  00 01 00                   .".....Z ...
    00000000  0f 22 00 00 00 11 01 5a  00 fe fa 00 00 01 00 00   .".....Z ........
    00000010  14 00 00 00 00 00 00                              .......
0000000B  0f 23 00 00 00 04 01 5a  00 11                      .#.....Z ..
    00000017  0f 23 00 00 00 04 01 5a  00 fe                     .#.....Z ..
00000015  0f 24 00 00 00 28 01 5a  00 10 00 00 00 00 00 00    .$...(.Z ........
00000025  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00000035  00 00 00 00 00 00 00 00  00 00 00 00 00 00          ........ ......
    00000021  0f 24 00 00 00 05 01 5a  00 fe 26                  .$.....Z ..&
00000043  0f 25 00 00 00 09 01 5a  00 6d 08 d3 f8 6f 8d       .%.....Z .m...o.
    0000002C  0f 25 00 00 00 05 01 5a  00 fd 83                  .%.....Z ...
00000052  0f 26 00 00 00 04 01 5a  26 12                      .&.....Z &.
    00000037  0f 26 00 00 00 04 01 5a  26 fe                     .&.....Z &.
0000005C  0f 27 00 00 00 04 01 5a  00 02                      .'.....Z ..
    00000041  0f 27 00 00 00 30 01 5a  00 fe 14 30 87 07 00 00   .'...0.Z ...0....
    00000051  00 00 01 00 06 01 01 00  07 00 00 00 ff ff 00 00   ........ ........
    00000061  11 54 4d 32 32 31 43 45  31 36 52 20 20 00 00 00   .TM221CE 16R  ...
    00000071  01 6e ff 01 87 00                                 .n....
00000066  0f 28 00 00 00 04 01 5a  00 02                      .(.....Z ..
    00000077  0f 28 00 00 00 30 01 5a  00 fe 14 30 87 07 00 00   .(...0.Z ...0....
    00000087  00 00 01 00 06 01 01 00  07 00 00 00 ff ff 00 00   ........ ........
    00000097  11 54 4d 32 32 31 43 45  31 36 52 20 20 00 00 00   .TM221CE 16R  ...
    000000A7  01 6e ff 01 87 00                                 .n....
00000070  0f 29 00 00 00 04 01 5a  00 04                      .).....Z ..
    000000AD  0f 29 00 00 00 1a 01 5a  00 fe 03 0a 80 03 68 42   .).....Z ......hB
    000000BD  bf 5e 68 42 bf 5e db 5d  ff ff 01 03 00 14 00 00   .^hB.^.] ........
0000007A  0f 2a 00 00 00 04 01 5a  00 04                      .*.....Z ..
    000000CD  0f 2a 00 00 00 1a 01 5a  00 fe 03 0a 80 03 68 42   .*.....Z ......hB
    000000DD  bf 5e 68 42 bf 5e db 5d  ff ff 01 03 00 14 00 00   .^hB.^.] ........
00000084  0f 2b 00 00 00 04 01 5a  00 04                      .+.....Z ..
    000000ED  0f 2b 00 00 00 1a 01 5a  00 fe 03 0a 80 03 68 42   .+.....Z ......hB
    000000FD  bf 5e 68 42 bf 5e db 5d  ff ff 01 03 00 14 00 00   .^hB.^.] ........
```

Figure 20: Modbus TCP communication between 192.168.10.164 and 192.168.10.45



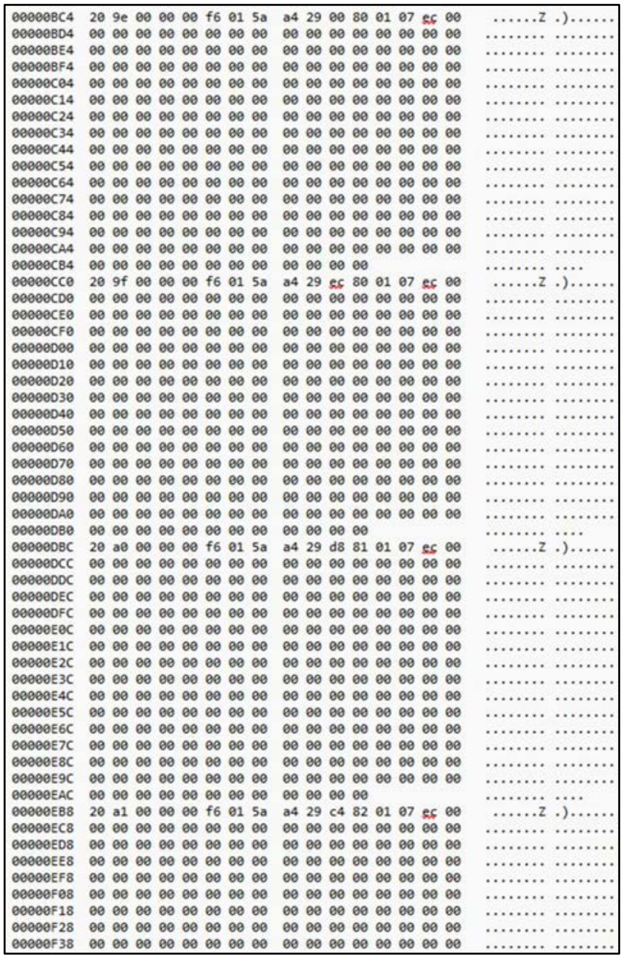
```
0000070E  0f 5c 00 00 00 f6 01 5a  26 29 00 80 01 07 ec 00   .\.....Z &)......
0000071E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000072E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000073E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000074E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000075E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000076E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000077E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000078E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000079E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007AE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007BE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007CE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007DE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007EE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000007FE  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
    000007C1  0f 5c 00 00 00 04 01 5a  26 fe                      .\.....Z &.
```

Figure 21: Frame # 186, Modbus TCP communication between 192.168.10.164 and 192.168.10.45

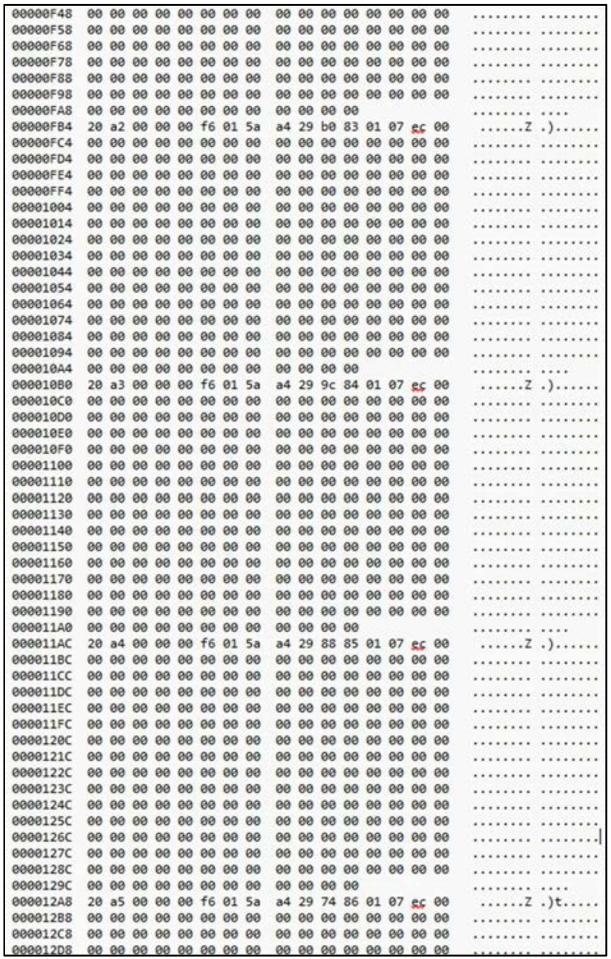
We have calculated the time of intervention as defined in section 3.4. We have used following calculation to determine the time window:

Assumed time of intervention is between 14:50:14 to 15:05:19
On-Chip PLC Backup 2 and 3 is: 14:50:07 to 15:05:09
Jitter Assumption 1 sec
∴ Considered time frame: 14:50:06 to 15:05:20
∴ The selected frames for investigation from Network Log: 31314 to 58579

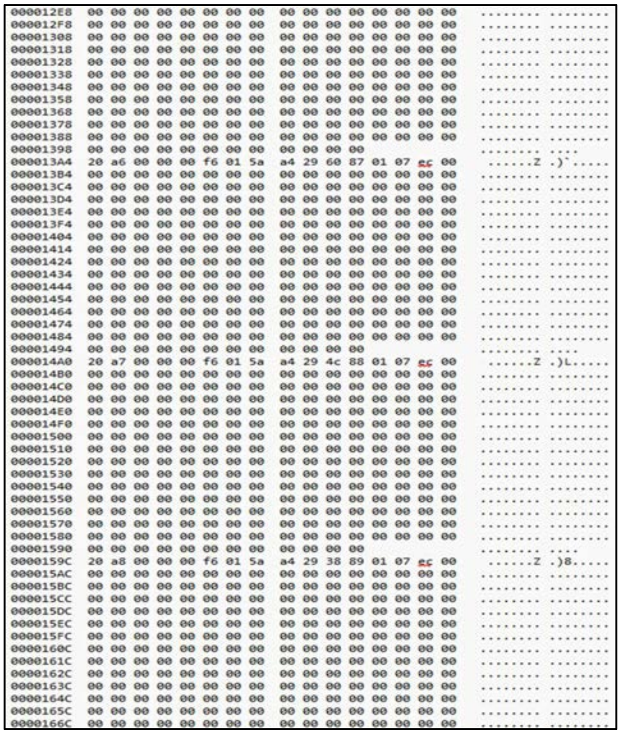
We found the frame number 46835 – 47267 started a suspicious session and uploaded suspicious instructions to the PLC. In this case the source IP is 192.168.10.164 and the destination is the PLC system of IP 192.168.45. Figure 22 shows the decoded Modbus TCP.



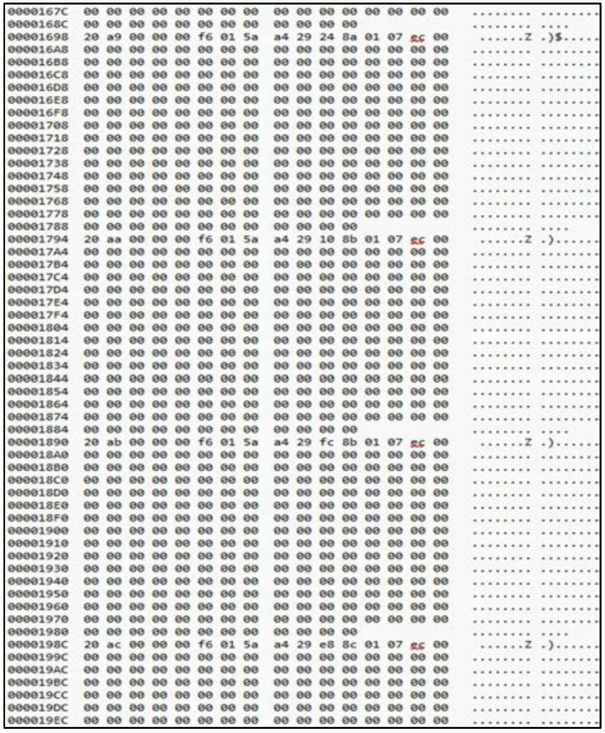
```
00000BC4  20 9e 00 00 00 f6 01 5a  a4 29 00 80 01 07 ec 00    ......Z .)......
00000BD4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000BE4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000BF4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C04  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C14  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C24  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C34  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C44  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C54  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C64  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C74  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C84  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000C94  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000CA4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000CB4  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00000CC0  20 9f 00 00 00 f6 01 5a  a4 29 ec 80 01 07 ec 00    ......Z .)......
00000CD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000CE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000CF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000D90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000DA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000DB0  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00000DBC  20 a0 00 00 00 f6 01 5a  a4 29 d8 81 01 07 ec 00    ......Z .)......
00000DCC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000DDC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000DEC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000DFC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E0C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E1C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E2C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E3C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E4C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E5C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E6C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E7C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E8C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000E9C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000EAC  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00000EB8  20 a1 00 00 00 f6 01 5a  a4 29 c4 82 01 07 ec 00    ......Z .)......
00000EC8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000ED8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000EE8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000EF8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F08  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F18  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F28  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F38  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```



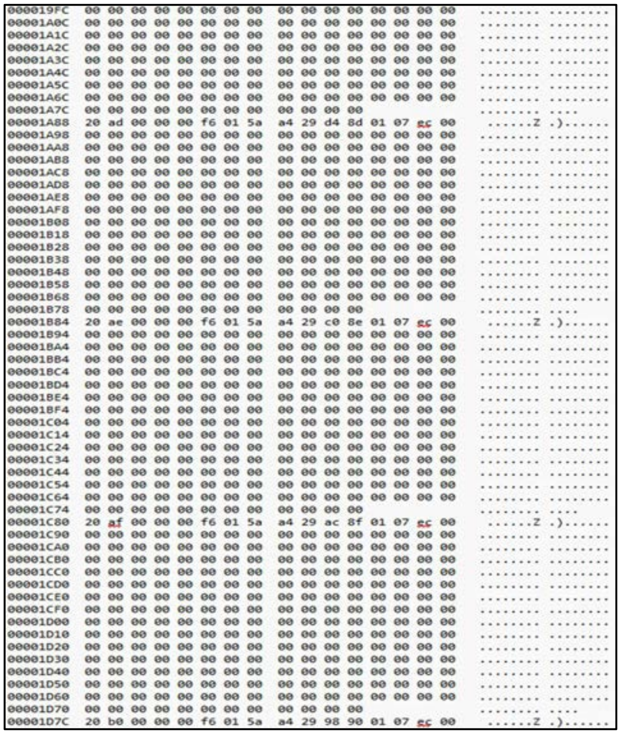
```
00000F48  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F68  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F78  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F88  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000F98  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000FA8  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00000FB4  20 a2 00 00 00 f6 01 5a  a4 29 b0 83 01 07 ec 00    ......Z .)......
00000FC4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000FD4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000FE4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00000FF4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001004  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001014  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001024  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001034  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001044  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001054  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001064  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001074  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001084  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001094  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000010A4  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
000010B0  20 a3 00 00 00 f6 01 5a  a4 29 9c 84 01 07 ec 00    ......Z .)......
000010C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000010D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000010E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000010F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000011A0  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
000011AC  20 a4 00 00 00 f6 01 5a  a4 29 88 85 01 07 ec 00    ......Z .)......
000011BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000011CC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000011DC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000011EC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000011FC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000120C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000121C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000122C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000123C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000124C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000125C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000126C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000127C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000128C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000129C  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
000012A8  20 a5 00 00 00 f6 01 5a  a4 29 74 86 01 07 ec 00    ......Z .)t.....
000012B8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000012C8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000012D8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```



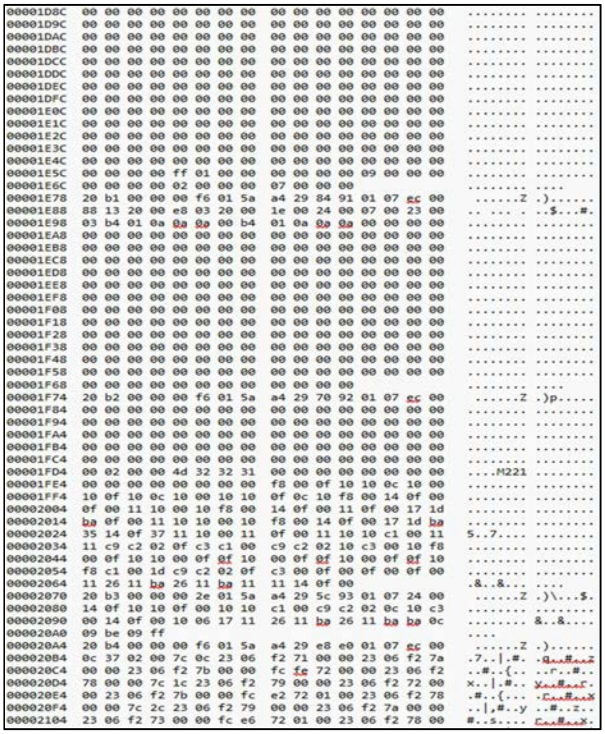
```
000012E8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000012F8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001308  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001318  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001328  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001338  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001348  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001358  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001368  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001378  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001388  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001398  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
000013A4  20 a6 00 00 00 f6 01 5a  a4 29 60 87 01 07 ec 00    ......Z .)`.....
000013B4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000013C4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000013D4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000013E4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000013F4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001404  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001414  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001424  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001434  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001444  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001454  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001464  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001474  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001484  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001494  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
000014A0  20 a7 00 00 00 f6 01 5a  a4 29 4c 88 01 07 ec 00    ......Z .)L.....
000014B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000014C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000014D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000014E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000014F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001500  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001510  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001520  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001530  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001540  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001550  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001570  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001580  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001590  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
0000159C  20 a8 00 00 00 f6 01 5a  a4 29 38 89 01 07 ec 00    ......Z .)8.....
000015AC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000015BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000015CC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000015DC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000015EC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000015FC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000160C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000161C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000162C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000163C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000164C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000165C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000166C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```



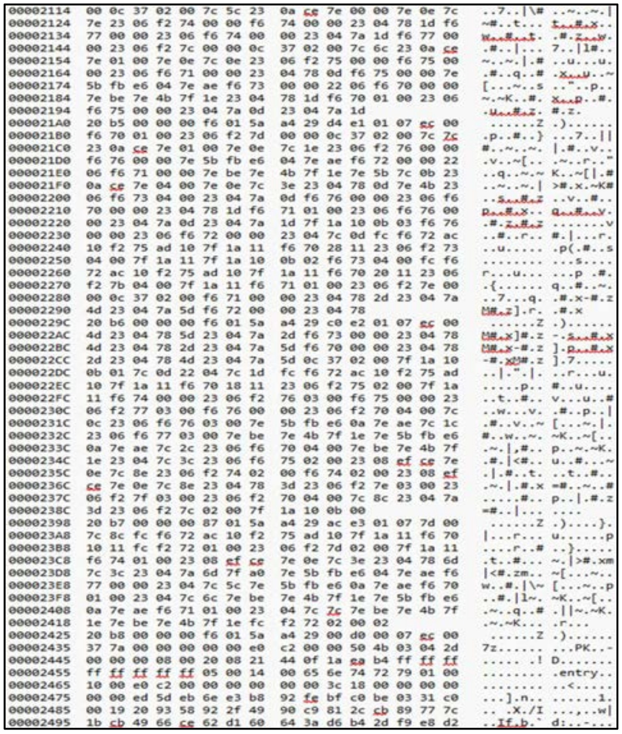
```
0000167C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000168C  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001698  20 a9 00 00 00 f6 01 5a  a4 29 24 8a 01 07 ec 00    ......Z .)$.....
000016A8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000016B8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000016C8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000016D8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000016E8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000016F8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001708  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001718  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001728  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001738  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001748  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001758  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001768  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001778  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001788  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001794  20 aa 00 00 00 f6 01 5a  a4 29 10 8b 01 07 ec 00    ......Z .)......
000017A4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000017B4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000017C4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000017D4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000017E4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000017F4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001804  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001814  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001824  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001834  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001844  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001854  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001864  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001874  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001884  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001890  20 ab 00 00 00 f6 01 5a  a4 29 fc 8b 01 07 ec 00    ......Z .)......
000018A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000018B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000018C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000018D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000018E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000018F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001900  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001910  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001920  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001930  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001940  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001950  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001960  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001970  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001980  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
0000198C  20 ac 00 00 00 f6 01 5a  a4 29 e8 8c 01 07 ec 00    ......Z .)......
0000199C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000019AC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000019BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000019CC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000019DC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000019EC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```



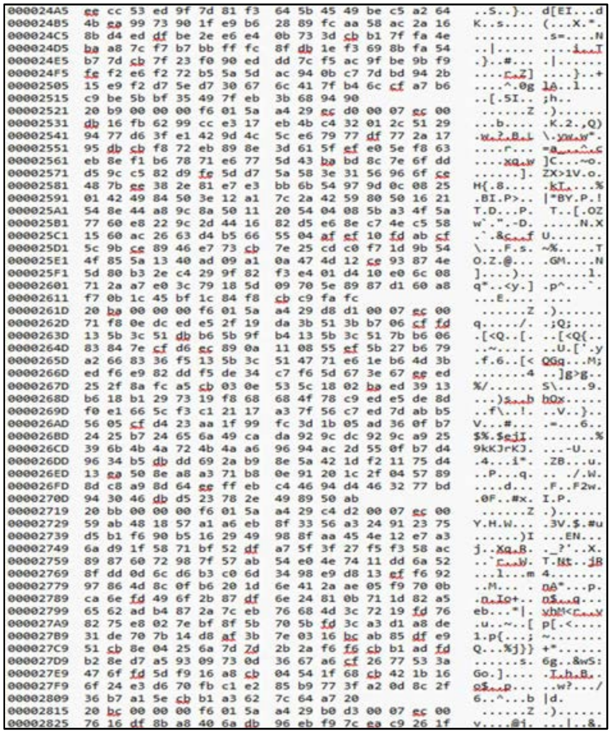
```
000019FC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A0C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A1C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A2C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A3C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A4C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A5C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A6C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001A7C  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001A88  20 ad 00 00 00 f6 01 5a  a4 29 d4 8d 01 07 ec 00    ......Z .)......
00001A98  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AA8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AB8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AC8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AD8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AE8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001AF8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B08  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B18  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B28  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B38  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B48  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B68  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001B78  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001B84  20 ae 00 00 00 f6 01 5a  a4 29 c0 8e 01 07 ec 00    ......Z .)......
00001B94  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BA4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BB4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BC4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BD4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BE4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001BF4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C04  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C14  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C24  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C34  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C44  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C54  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C64  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001C74  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001C80  20 af 00 00 00 f6 01 5a  a4 29 ac 8f 01 07 ec 00    ......Z .)......
00001C90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001CF0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D70  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001D7C  20 b0 00 00 00 f6 01 5a  a4 29 98 90 01 07 ec 00    ......Z .)......
```



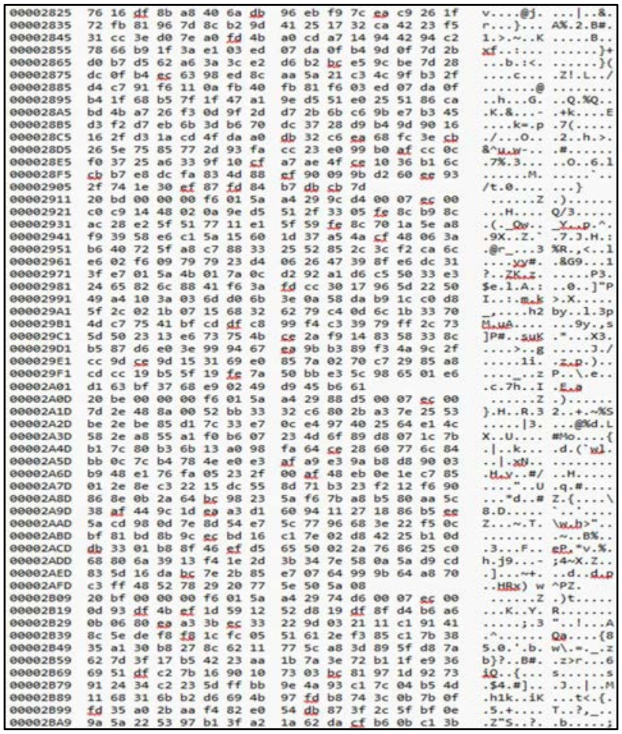
```
00001D8C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001D9C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DAC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DBC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DCC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DDC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DEC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001DFC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E0C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E1C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E2C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E3C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E4C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001E5C  00 00 00 00 ff 01 00 00  00 00 00 00 09 00 00 00   ........ ........
00001E6C  00 00 00 00 02 00 00 00  07 00 00 00               ........ ....
00001E78  20 b1 00 00 00 f6 01 5a  a4 29 84 91 01 07 ec 00    ......Z .)......
00001E88  88 13 20 00 e8 03 20 00  1e 00 24 00 07 00 23 00   .. ... . ..$...#.
00001E98  03 b4 01 0a 0a 0a 00 b4  01 0a 0a 0a 00 00 00 00   ........ ........
00001EA8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001EB8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001EC8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001ED8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001EE8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001EF8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F08  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F18  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F28  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F38  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F48  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F58  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F68  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00001F74  20 b2 00 00 00 f6 01 5a  a4 29 70 92 01 07 ec 00    ......Z .)p.....
00001F84  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001F94  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001FA4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001FB4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001FC4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00001FD4  00 02 00 00 4d 32 32 31  00 00 00 00 00 00 00 00   ....M221 ........
00001FE4  00 00 00 00 00 00 00 00  f8 00 0f 10 10 0c 10 00   ........ ........
00001FF4  10 0f 10 0c 10 00 10 10  0f 0c 10 f8 00 14 0f 00   ........ ........
00002004  0f 00 11 10 00 10 f8 00  14 0f 00 11 0f 00 17 1d   ........ ........
00002014  ba 0f 00 11 10 10 00 10  f8 00 14 0f 00 17 1d ba   ........ ........
00002024  35 14 0f 37 11 10 00 11  0f 00 11 10 10 c1 00 11   5..7.... ........
00002034  11 c9 c2 02 0f c3 c1 00  c9 c2 02 10 c3 00 10 f8   ........ ........
00002044  00 0f 10 10 00 0f 0f 10  00 0f 0f 10 00 0f 0f 10   ........ ........
00002054  f8 c1 00 1d c9 c2 02 0f  c3 00 0f 00 0f 00 0f 00   ........ ........
00002064  11 26 11 ba 26 11 ba 11  11 14 0f 00               .&..&... ....
00002070  20 b3 00 00 00 2e 01 5a  a4 29 5c 93 01 07 24 00    ......Z .)\...$.
00002080  14 0f 10 10 0f 00 10 10  c1 00 c9 c2 02 0c 10 c3   ........ ........
00002090  00 14 0f 00 10 06 17 11  26 11 ba 26 11 ba ba 0c   ........ &..&....
000020A0  09 be 09 ff                                        ....
000020A4  20 b4 00 00 00 f6 01 5a  a4 29 e8 e0 01 07 ec 00    ......Z .)......
000020B4  0c 37 02 00 7c 0c 23 06  f2 71 00 00 23 06 f2 7a   .7..|.#. .q..#..z
000020C4  00 00 23 06 f2 7b 00 00  fc fe 72 00 00 23 06 f2   ..#..{.. ..r..#..
000020D4  78 00 00 7c 1c 23 06 f2  79 00 00 23 06 f2 72 00   x..|.#.. y..#..r.
000020E4  00 23 06 f2 7b 00 00 fc  e2 72 01 00 23 06 f2 78   .#..{... .r..#..x
000020F4  00 00 7c 2c 23 06 f2 79  00 00 23 06 f2 7a 00 00   ..|,#..y ..#..z..
00002104  23 06 f2 73 00 00 fc e6  72 01 00 23 06 f2 78 00   #..s.... r..#..x.
```



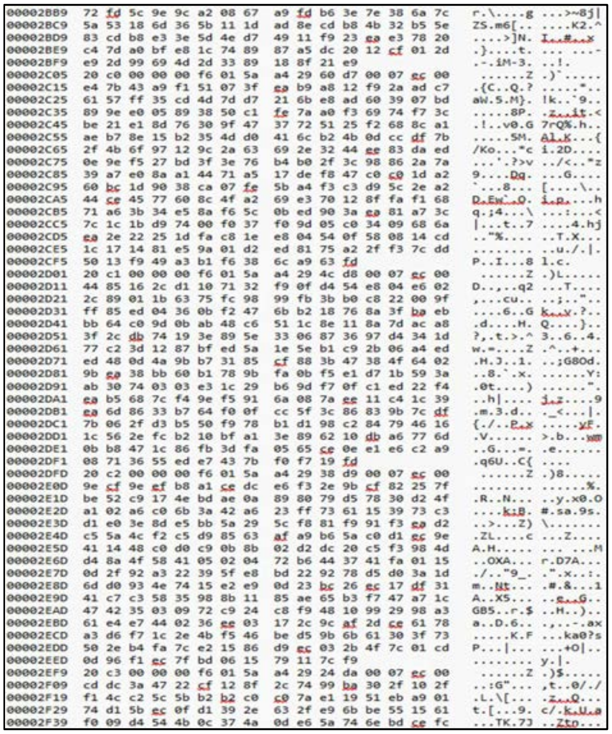
```
00002114  00 0c 37 02 00 7c 5c 23  0a ce 7e 00 00 7e 0e 7c   ..7..|\# ..~..~.|
00002124  7e 23 06 f2 74 00 00 f6  74 00 00 23 04 78 1d f6   ~#..t... t..#.x..
00002134  77 00 00 23 06 f6 74 00  00 23 04 7a 1d f6 77 00   w..#..t. .#.z..w.
00002144  00 23 06 f2 7c 00 00 0c  37 02 00 7c 6c 23 0a ce   .#..|... 7..|l#..
00002154  7e 01 00 7e 0e 7c 0e 23  06 f2 75 00 00 f6 75 00   ~..~.|.# ..u...u.
00002164  00 23 06 f6 71 00 00 23  04 78 0d f6 75 00 00 7e   .#..q..# .x..u..~
00002174  5b fb e6 04 7e ae f6 73  00 00 22 06 f6 70 00 00   [...~..s .."..p..
00002184  7e be 7e 4b 7f 1e 23 04  78 1d f6 70 01 00 23 06   ~.~K..#. x..p..#.
00002194  f6 75 00 00 23 04 7a 0d  23 04 7a 1d               .u..#.z. #.z.
000021A0  20 b5 00 00 00 f6 01 5a  a4 29 d4 e1 01 07 ec 00    ......Z .)......
000021B0  f6 70 01 00 23 06 f2 7d  00 00 0c 37 02 00 7c 7c   .p..#..} ...7..||
000021C0  23 0a ce 7e 01 00 7e 0e  7c 1e 23 06 f2 76 00 00   #..~..~. |.#..v..
000021D0  f6 76 00 00 7e 5b fb e6  04 7e ae f6 72 00 00 22   .v..~[.. .~..r.."
000021E0  06 f6 71 00 00 7e be 7e  4b 7f 1e 7e 5b 7c 0b 23   ..q..~.~ K..~[|.#
000021F0  0a ce 7e 04 00 7e 0e 7c  3e 23 04 78 0d 7e 4b 23   ..~..~.| >#.x.~K#
00002200  06 f6 73 04 00 23 04 7a  0d f6 76 00 00 23 06 f6   ..s..#.z ..v..#..
00002210  70 00 00 23 04 78 1d f6  71 01 00 23 06 f6 76 00   p..#.x.. q..#..v.
00002220  00 23 04 7a 0d 23 04 7a  1d 7f 1a 10 0b 03 f6 76   .#.z.#.z .......v
00002230  00 00 23 06 f6 72 00 00  23 04 7c 0d fc f6 72 ac   ..#..r.. #.|...r.
00002240  10 f2 75 ad 10 7f 1a 11  f6 70 28 11 23 06 f2 73   ..u..... .p(.#..s
00002250  04 00 7f 1a 11 7f 1a 10  0b 02 f6 73 04 00 fc f6   ........ ...s....
00002260  72 ac 10 f2 75 ad 10 7f  1a 11 f6 70 20 11 23 06   r...u... ...p .#.
00002270  f2 7b 04 00 7f 1a 11 f6  71 01 00 23 06 f2 7e 00   .{...... q..#..~.
00002280  00 0c 37 02 00 f6 71 00  00 23 04 78 2d 23 04 7a   ..7...q. .#.x-#.z
00002290  4d 23 04 7a 5d f6 72 00  00 23 04 78               M#.z].r. .#.x
0000229C  20 b6 00 00 00 f6 01 5a  a4 29 c0 e2 01 07 ec 00    ......Z .)......
000022AC  4d 23 04 78 5d 23 04 7a  2d f6 73 00 00 23 04 78   M#.x]#.z -.s..#.x
000022BC  4d 23 04 78 2d 23 04 7a  5d f6 70 00 00 23 04 78   M#.x-#.z ].p..#.x
000022CC  2d 23 04 78 4d 23 04 7a  5d 0c 37 02 00 7f 1a 10   -#.xM#.z ].7.....
000022DC  0b 01 7c 0d 22 04 7c 1d  fc f6 72 ac 10 f2 75 ad   ..|.".|. ..r...u.
000022EC  10 7f 1a 11 f6 70 18 11  23 06 f2 75 02 00 7f 1a   .....p.. #..u....
000022FC  11 f6 74 00 00 23 06 f2  76 03 00 f6 75 00 00 23   ..t..#.. v...u..#
0000230C  06 f2 77 03 00 f6 76 00  00 23 06 f2 70 04 00 7c   ..w...v. .#..p..|
0000231C  0c 23 06 f6 76 03 00 7e  5b fb e6 0a 7e ae 7c 1c   .#..v..~ [...~.|.
0000232C  23 06 f6 77 03 00 7e be  7e 4b 7f 1e 7e 5b fb e6   #..w..~. ~K..~[..
0000233C  0a 7e ae 7c 2c 23 06 f6  70 04 00 7e be 7e 4b 7f   .~.|,#.. p..~.~K.
0000234C  1e 23 04 7c 3c 23 06 f6  75 02 00 23 08 ef ce 7e   .#.|<#.. u..#...~
0000235C  0e 7c 8e 23 06 f2 74 02  00 f6 74 02 00 23 08 ef   .|.#..t. ..t..#..
0000236C  ce 7e 0e 7c 8e 23 04 78  3d 23 06 f2 7e 03 00 23   .~.|.#.x =#..~..#
0000237C  06 f2 7f 03 00 23 06 f2  70 04 00 7c 8c 23 04 7a   .....#.. p..|.#.z
0000238C  3d 23 06 f2 7c 02 00 7f  1a 10 0b 00               =#..|... ....
00002398  20 b7 00 00 00 87 01 5a  a4 29 ac e3 01 07 7d 00    ......Z .)....}.
000023A8  7c 8c fc f6 72 ac 10 f2  75 ad 10 7f 1a 11 f6 70   |...r... u......p
000023B8  10 11 fc f2 72 01 00 23  06 f2 7d 02 00 7f 1a 11   ....r..# ..}.....
000023C8  f6 74 01 00 23 08 ef ce  7e 0e 7c 3e 23 04 78 6d   .t..#... ~.|>#.xm
000023D8  7c 3c 23 04 7a 6d 7f a0  7e 5b fb e6 04 7e ae f6   |<#.zm.. ~[...~..
000023E8  77 00 00 23 04 7c 5c 7e  5b fb e6 0a 7e ae f6 70   w..#.|\~ [...~..p
000023F8  01 00 23 04 7c 6c 7e be  7e 4b 7f 1e 7e 5b fb e6   ..#.|l~. ~K..~[..
00002408  0a 7e ae f6 71 01 00 23  04 7c 7c 7e be 7e 4b 7f   .~..q..# .||~.~K.
00002418  1e 7e be 7e 4b 7f 1e fc  f2 72 02 00 02            .~.~K... .r...
00002425  20 b8 00 00 00 f6 01 5a  a4 29 00 d0 00 07 ec 00    ......Z .)......
00002435  37 7a 00 00 00 00 00 e0  c2 00 00 50 4b 03 04 2d   7z...... ...PK..-
00002445  00 00 00 08 00 20 08 21  44 0f 1a ea b4 ff ff ff   ..... .! D.......
00002455  ff ff ff ff ff 05 00 14  00 65 6e 74 72 79 01 00   ........ .entry..
00002465  10 00 e0 c2 00 00 00 00  00 00 3c 18 00 00 00 00   ........ ..<.....
00002475  00 00 ed 5d eb 6e e3 b8  92 fe bf c0 be 03 31 c0   ...].n.. ......1.
00002485  00 19 20 93 58 92 2f 49  90 c9 81 2c cb 89 77 7c   .. .X./I ...,..w|
00002495  1b cb 49 66 ce 62 d1 60  64 3a d6 b4 2d f9 e8 d2   ..If.b.` d:..-...
```



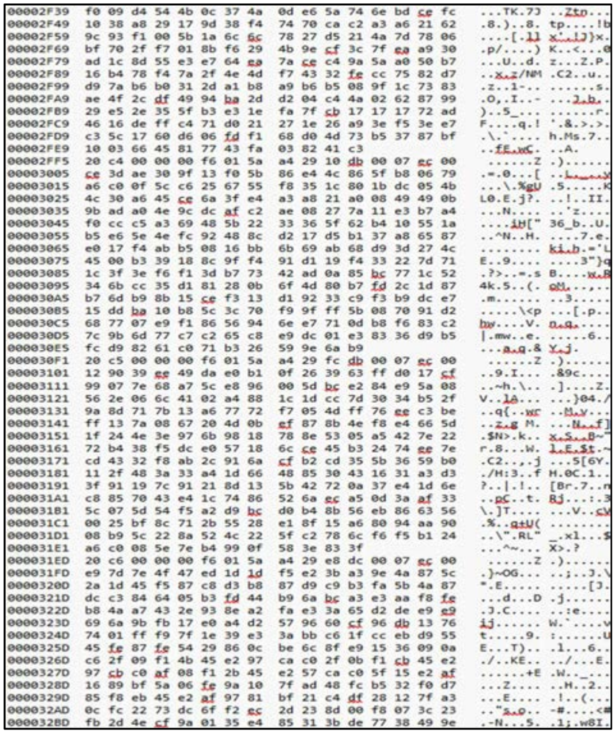
```
000024A5  ee cc 53 ed 9f 7d 81 f3  64 5b 45 49 be c5 a2 64   ..S..}.. d[EI...d
000024B5  4b ea 99 73 90 1f e9 b6  28 89 fc aa 58 ac 2a 16   K..s.... (...X.*.
000024C5  8b d4 ed df be 2e e6 e4  0b 73 3d cb b1 7f fa 4e   ........ .s=....N
000024D5  ba a8 7c f7 b7 bb ff fc  8f db 1e f3 69 8b fa 54   ..|..... ....i..T
000024E5  b7 7d cb 7f 23 f0 90 ed  dd 7c f5 ac 9f be 9b f9   .}..#... .|......
000024F5  fe f2 e6 f2 72 b5 5a 5d  ac 94 0b c7 7d bd 94 2b   ....r.Z] ....}..+
00002505  15 e9 f2 d7 5e d7 30 67  6c 41 7f b4 6c cf a7 b6   ....^.0g lA..l...
00002515  c9 be 5b bf 35 49 7f eb  3b 68 94 90               ..[.5I.. ;h..
00002521  20 b9 00 00 00 f6 01 5a  a4 29 ec d0 00 07 ec 00    ......Z .)......
00002531  db 16 fb 62 99 cc e3 17  eb 4b c4 32 01 2c 51 29   ...b.... .K.2.,Q)
00002541  94 77 d6 3f e1 42 9d 4c  5c e6 79 77 df 77 2a 17   .w.?.B.L \.yw.w*.
00002551  95 db cb f8 72 eb 89 8e  3d 61 5f ef e0 5e f8 63   ....r... =a_..^.c
00002561  eb 8e f1 b6 78 71 e6 77  5d 43 ba bd 8c 7e 6f dd   ....xq.w ]C...~o.
00002571  d5 9c c5 82 d9 fe 5d d7  5a 58 3e 31 56 96 6f ce   ......]. ZX>1V.o.
00002581  48 7b ee 38 2e 81 e7 e3  bb 6b 54 97 9d 0c 08 25   H{.8.... .kT....%
00002591  01 42 49 84 50 3e 12 a1  7c 2a 42 59 80 50 16 21   .BI.P>.. |*BY.P.!
000025A1  54 8e 44 a8 9c 8a 50 11  20 54 04 08 5b a3 4f 5a   T.D...P.  T..[.OZ
000025B1  77 60 e8 22 9c 2d 44 16  82 d5 e6 8e c7 4e c5 58   w`.".-D. .....N.X
000025C1  15 60 ac 26 63 d4 b5 66  55 04 af ef 10 fd ab cf   .`.&c..f U.......
000025D1  5c 9b ce 89 46 e7 73 cb  7e 25 cd c0 f7 1d 9b 54   \...F.s. ~%.....T
000025E1  4f 85 5a 13 40 ad 09 a1  0a 47 4d 12 ce 93 87 4e   O.Z.@... .GM....N
000025F1  5d 80 b3 2e c4 29 9f 82  f3 e4 01 d4 10 e0 6c 08   ]....).. ......l.
00002601  71 2a a7 e0 3c 79 18 5d  09 70 5e 89 87 d1 60 a8   q*..<y.] .p^...`.
00002611  f7 0b 1c 45 bf 1c 84 f8  cb c9 fa fc               ...E.... ....
0000261D  20 ba 00 00 00 f6 01 5a  a4 29 d8 d1 00 07 ec 00    ......Z .)......
0000262D  71 f8 0e dc ed e5 2f 19  da 3b 51 3b b7 06 cf fd   q...../. .;Q;....
0000263D  13 5b 3c 51 db b6 5b 9f  b4 13 5b 3c 51 7b b6 06   .[<Q..[. ..[<Q{..
0000264D  83 84 7e cf d6 ec 89 0a  11 08 55 ef 5b 27 b6 79   ..~..... ..U.['.y
0000265D  a2 66 83 36 f5 13 5b 3c  51 47 71 e6 1e b6 4d 3b   .f.6..[< QGq...M;
0000266D  ed f6 e9 82 dd f5 de 34  c7 f6 5d 67 3e 67 ee ed   .......4 ..]g>g..
0000267D  25 2f 8a fc a5 cb 03 0e  53 5c 18 02 ba ed 39 13   %/...... S\....9.
0000268D  b6 18 b1 29 73 19 f8 68  68 4f 78 c9 ed e5 de 8d   ...)s..h hOx.....
0000269D  f0 e1 66 5c f3 c1 21 17  a3 7f 56 c7 ed 7d ab b5   ..f\..!. ..V..}..
000026AD  56 05 cf d4 23 aa 1f 99  fc 3d 1b 05 ad 36 0f b7   V...#... .=...6..
000026BD  24 25 b7 24 65 6a 49 ca  da 92 9c dc 92 9c a9 25   $%.$ejI. .......%
000026CD  39 6b 4b 4a 72 4b 4a a6  96 94 ac 2d 55 0f b7 d4   9kKJrKJ. ...-U...
000026DD  96 34 b5 db dd 69 2a b9  8e 5a 42 1d f2 11 75 d4   .4...i*. .ZB...u.
000026ED  13 ea 50 8e a8 a3 71 b8  0e 91 20 1c 2f 04 57 89   ..P...q. .. ./.W.
000026FD  8d c8 a9 8d 64 ee ff eb  c4 46 94 d4 46 32 77 bd   ....d... .F..F2w.
0000270D  94 30 46 db d5 23 78 2e  49 89 50 ab               .0F..#x. I.P.
00002719  20 bb 00 00 00 f6 01 5a  a4 29 c4 d2 00 07 ec 00    ......Z .)......
00002729  59 ab 48 18 57 a1 a6 eb  8f 33 56 a3 24 91 23 75   Y.H.W... .3V.$.#u
00002739  d5 b1 f6 90 b5 16 29 49  98 8f aa 45 4e 12 e7 a3   ......)I ...EN...
00002749  6a d9 1f 58 71 bf 52 df  a7 5f 3f 27 f5 f3 58 ac   j..Xq.R. ._?'..X.
00002759  89 87 60 72 98 7f 57 ab  54 e0 4e 74 11 dd 6a 52   ..`r..W. T.Nt..jR
00002769  8f dd 0d 6c d6 b3 c0 6d  34 98 e9 d8 13 ef f6 92   ...l...m 4.......
00002779  97 86 4d 8c 0f b6 20 1d  6e 41 2a ae 05 f9 70 0b   ..M... . nA*...p.
00002789  ca 6e fd 49 6f 2b 87 df  6e 24 81 0b 71 1d 82 a5   .n.Io+.. n$..q...
00002799  65 62 ad b4 87 2a 7c eb  76 68 4d 3c 72 19 fd 76   eb...*|. vhM<r..v
000027A9  82 75 e8 02 7e bf 8f 5b  70 5b fd 3c a3 d1 a8 de   .u..~..[ p[.<....
000027B9  31 de 70 7b 14 d8 af 3b  7e 03 16 bc ab 85 df e9   1.p{...; ~.......
000027C9  51 cb 8e 04 25 6a 7d 7d  2b 2a f6 f6 cb b1 ad fd   Q...%j}} +*......
000027D9  b2 8e d7 a5 93 09 73 0d  36 67 a6 cf 26 77 53 3a   ......s. 6g..&wS:
000027E9  47 6f fd 5d f9 16 a8 cb  04 54 1f 68 cb 42 1b 16   Go.].... .T.h.B..
000027F9  6f 24 e3 d6 70 fb c1 e2  85 b9 77 3f a2 0d 8c 2f   o$..p... ..w?.../
00002809  36 b7 a1 5e cb b1 a3 62  7c 64 a7 20               6..^...b |d.
00002815  20 bc 00 00 00 f6 01 5a  a4 29 b0 d3 00 07 ec 00    ......Z .)......
00002825  76 16 df 8b a8 40 6a db  96 eb f9 7c ea c9 26 1f   v....@j. ...|..&.
```



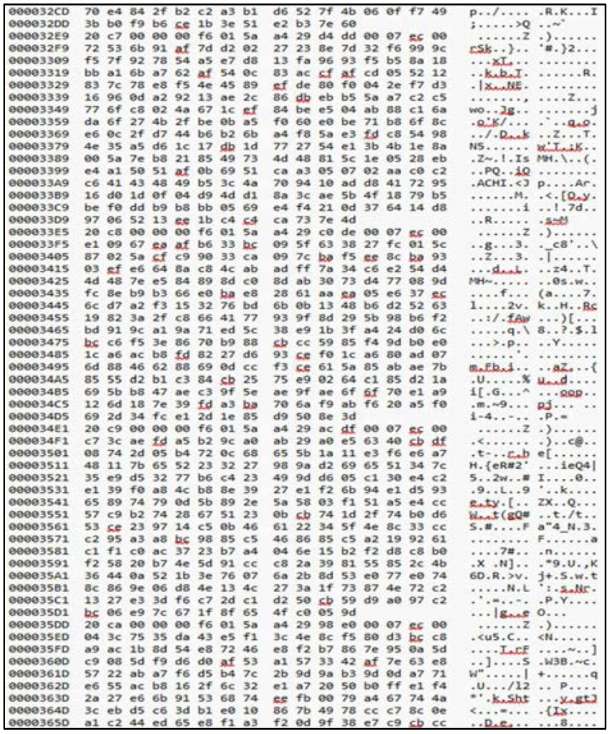
```
00002825  76 16 df 8b a8 40 6a db  96 eb f9 7c ea c9 26 1f   v....@j. ...|..&.
00002835  72 fb 81 96 7d 8c b2 9d  41 25 17 32 ca 42 23 f5   r...}... A%.2.B#.
00002845  31 cc 3e d0 7e a0 fd 4b  a0 cd a7 14 94 42 94 c2   1.>.~..K .....B..
00002855  78 66 b9 1f 3a e1 03 ed  07 da 0f b4 9d 0f 7d 2b   xf..:... ......}+
00002865  d0 b7 d5 62 a6 3a 3c e2  d6 b2 bc e5 9c be 7d 28   ...b.:<. ......}(
00002875  dc 0f b4 ec 63 98 ed 8c  aa 5a 21 c3 4c 9f b3 2f   ....c... .Z!.L../
00002885  d4 c7 91 f6 11 0a fb 40  fb 81 f6 03 ed 07 da 0f   .......@ ........
00002895  b4 1f 68 b5 7f 1f 47 a1  9e d5 51 e0 25 51 86 ca   ..h...G. ..Q.%Q..
000028A5  bd 4b a7 26 f3 0d 9f 2d  d7 2b 6b c6 9b e7 b3 45   .K.&...- .+k....E
000028B5  d3 f2 d7 eb 6b 3d b6 70  dc 37 28 d9 b4 9d 90 16   ....k=.p .7(.....
000028C5  16 2f d3 1a cd 4f da a0  db 32 c6 ea 68 fc 3e cb   ./...O.. .2..h.>.
000028D5  26 5e 75 85 77 2d 93 fa  cc 23 e0 99 b0 af cc 0c   &^u.w-.. .#......
000028E5  f0 37 25 a6 33 9f 10 cf  a7 ae 4f ce 10 36 b1 6c   .7%.3... ..O..6.l
000028F5  cb b7 e8 dc fa 83 4d 88  ef 90 09 9b d2 60 ee 93   ......M. .....`..
00002905  2f 74 1e 30 ef 87 fd 84  b7 db cb 7d               /t.0.... ...}
00002911  20 bd 00 00 00 f6 01 5a  a4 29 9c d4 00 07 ec 00    ......Z .)......
00002921  c0 c9 14 48 02 0a 9e d5  51 2f 33 05 fe 8c b9 8c   ...H.... Q/3.....
00002931  ac 28 e2 5f 51 77 11 e1  5f 59 fe 8c 70 1a 5e a8   .(._Qw.. _Y..p.^.
00002941  f9 39 58 e6 c1 5a 15 60  1d 37 a5 4a cf 48 06 3a   .9X..Z.` .7.J.H.:
00002951  b6 40 72 5f a8 c7 88 33  25 52 85 2c 3c f2 ca 6c   .@r_...3 %R.,<..l
00002961  e6 02 f6 09 79 79 23 d4  06 26 47 39 8f e6 dc 31   ....yy#. .&G9...1
00002971  3f e7 01 5a 4b 01 7a 0c  d2 92 a1 d6 c5 50 33 e3   ?..ZK.z. .....P3.
00002981  24 65 82 6c 88 41 f6 3a  fd cc 30 17 96 5d 22 50   $e.l.A.: ..0..]"P
00002991  49 a4 10 3a 03 6d d0 6b  3e 0a 58 da b9 1c c0 d8   I..:.m.k >.X.....
000029A1  5f 2c 02 1b 07 15 68 32  62 79 c4 0d 6c 1b 33 70   _,....h2 by..l.3p
000029B1  4d c7 75 41 bf cd df c8  99 f4 c3 39 79 ff 2c 73   M.uA.... ...9y.,s
000029C1  5d 50 23 13 e6 73 75 4b  ce 2a f9 14 83 58 33 8c   ]P#..suK .*...X3.
000029D1  b5 87 d6 e0 3e 99 94 67  ea 9b b3 89 f3 4a 9c 2f   ....>..g .....J./
000029E1  cc 9d ce 9d 15 31 69 e0  85 7a 02 70 c7 29 85 a8   .....1i. .z.p.)..
000029F1  cd cc 19 b5 5f 19 fe 7a  50 bb e3 5c 98 65 01 e6   ...._..z P..\.e..
00002A01  d1 63 bf 37 68 e9 02 49  d9 45 b6 61               .c.7h..I .E.a
00002A0D  20 be 00 00 00 f6 01 5a  a4 29 88 d5 00 07 ec 00    ......Z .)......
00002A1D  7d 2e 48 8a 00 52 bb 33  32 c6 80 2b a3 7e 25 53   }.H..R.3 2..+.~%S
00002A2D  be 2e be 85 d1 7c 33 e7  0c e4 97 40 25 64 e1 4c   .....|3. ...@%d.L
00002A3D  58 2e a8 55 a1 f0 b6 07  23 4d 6f 89 d8 07 1c 7b   X..U.... #Mo....{
00002A4D  b1 7c 80 b3 6b 13 a0 98  fa 64 ce 28 60 77 6c 84   .|..k... .d.(`wl.
00002A5D  bb 0c 7c b4 78 4e e0 e3  af a9 e3 9a b8 d8 90 03   ..|.xN.. ........
00002A6D  b9 48 e1 76 fa 05 23 2f  00 af 48 eb 0e 1e c7 85   .H.v..#/ ..H.....
00002A7D  01 2e 8e c3 22 15 dc 55  8d 71 b3 23 f2 12 f6 90   ...."..U .q.#....
00002A8D  86 8e 0b 2a 64 bc 98 23  5a f6 7b a8 b5 80 aa 5c   ...*d..# Z.{....\
00002A9D  38 af 44 9c 1d ea a3 d1  60 94 11 27 18 86 b5 ee   8.D..... `..'....
00002AAD  5a cd 98 0d 7e 8d 54 e7  5c 77 96 68 3e 22 f5 0c   Z...~.T. \w.h>"..
00002ABD  bf 81 bd 8b 9c ec bd 16  c1 7e 02 d8 42 25 b1 0d   ........ .~..B%..
00002ACD  db 33 01 b8 8f 46 ef d5  65 50 02 2a 76 86 25 c0   .3...F.. eP.*v.%.
00002ADD  68 80 6a 39 13 f4 1e 2d  3b 34 7e 58 0a 5a d9 cd   h.j9...- ;4~X.Z..
00002AED  83 5d 16 da bc 7e 2b 85  e7 07 64 99 9b 64 a8 70   .]...~+. ..d..d.p
00002AFD  c3 ff 48 52 78 29 20 77  5e 50 5a 08               ..HRx) w ^PZ.
00002B09  20 bf 00 00 00 f6 01 5a  a4 29 74 d6 00 07 ec 00    ......Z .)t.....
00002B19  0d 93 df 4b ef 1d 59 12  52 d8 19 df 8f d4 b6 a6   ...K..Y. R.......
00002B29  0b 06 80 ea a3 3b ec 33  22 9d 03 21 11 c1 91 41   .....;.3 "..!...A
00002B39  8c 5e de f8 f8 1c fc 05  51 61 2e f3 85 c1 7b 38   .^...... Qa....{8
00002B49  35 a1 30 b8 27 8c 62 11  77 5c a8 3d 89 5f d8 7a   5.0.'.b. w\.=._.z
00002B59  62 7d 3f 17 b5 42 23 aa  1b 7a 3e 72 b1 1f e9 36   b}?..B#. .z>r...6
00002B69  69 51 df c2 7b 16 90 10  73 03 bc 81 97 1d 92 73   iQ..{... s.......s
00002B79  91 24 34 c2 23 5d ff bb  9e 4a 93 c1 7c 04 b5 4d   .$4.#].. .J..|..M
00002B89  11 68 31 6b b2 d6 69 4b  97 fd b8 74 3c 0b 7b 0f   .h1k..iK ...t<.{.
00002B99  fd 35 a0 2b aa f4 82 e0  54 db 87 3f 2c 5f bf 0e   .5.+.... T..?,_..
00002BA9  9a 5a 22 53 97 b1 3f a2  1a 62 da cf b6 0b c1 3b   .Z"S..?. .b.....;
```



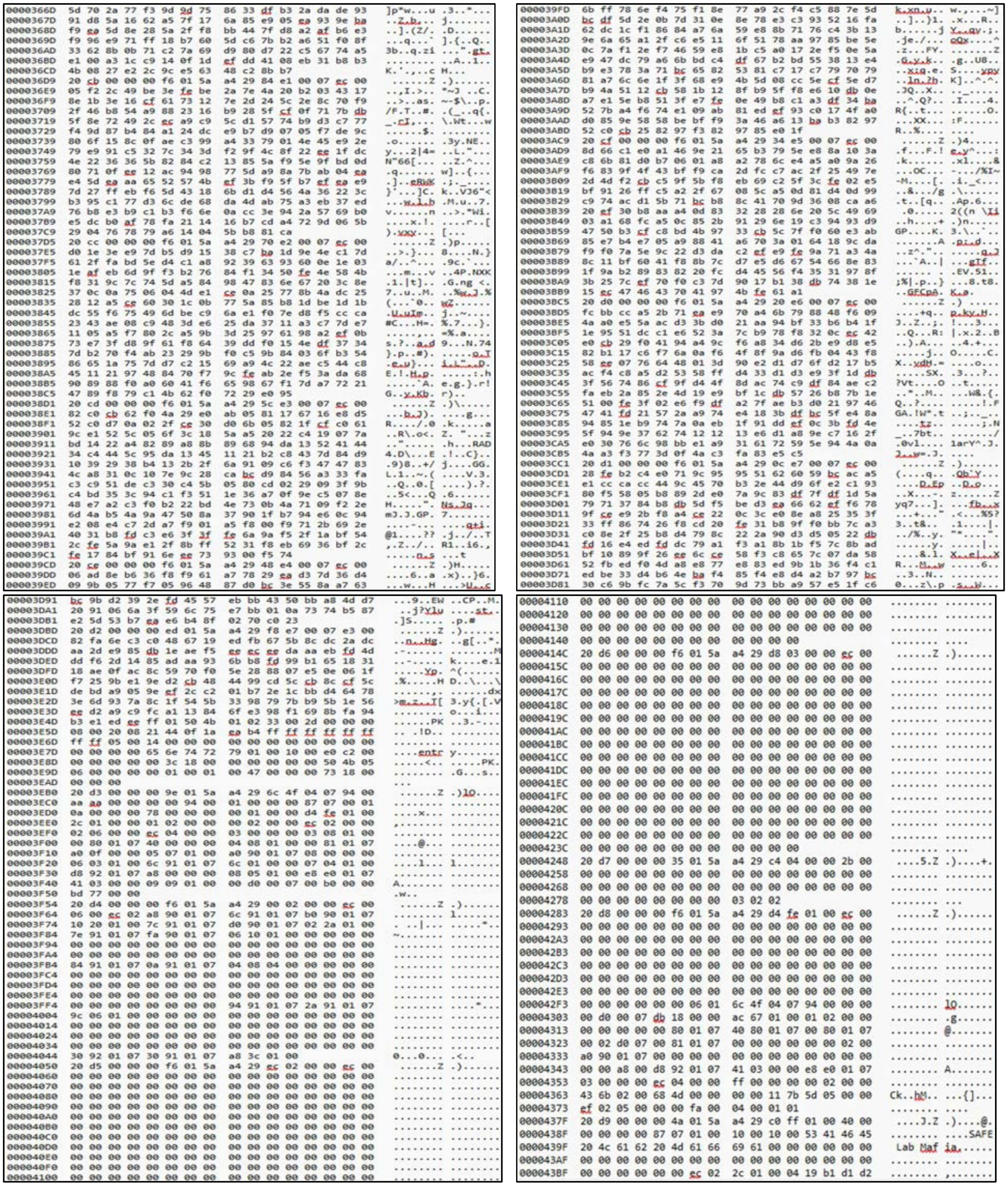
```
00002BB9  72 fd 5c 9e 9c a2 08 67  a9 fd b6 3e 7e 38 6a 7c   r.\....g ...>~8j|
00002BC9  5a 53 18 6d 36 5b 11 1d  ad 8e cd b8 4b 32 b5 5e   ZS.m6[.. ....K2.^
00002BD9  83 cd b8 e3 3e 5d 4e d7  49 11 f9 23 ea e3 78 20   ....>]N. I..#..x
00002BE9  c4 7d a0 bf e8 1c 74 89  87 a5 dc 20 12 cf 01 2d   .}....t. ... ...-
00002BF9  e9 2d 99 69 4d 2d 33 89  18 8f 21 e9               .-.iM-3. ..!.
00002C05  20 c0 00 00 00 f6 01 5a  a4 29 60 d7 00 07 ec 00    ......Z .)`.....
00002C15  e4 7b 43 a9 f1 51 07 3f  ea b9 a8 12 f9 2a ad c7   .{C..Q.? .....*..
00002C25  61 57 ff 35 cd 4d 7d d7  21 6b e8 ad 60 39 07 bd   aW.5.M}. !k..`9..
00002C35  89 9e e0 05 89 38 50 c1  fe 7a a0 f3 69 74 f7 3c   .....8P. .z..it.<
00002C45  be 21 e1 8d 76 30 9f 47  37 72 51 25 f2 68 8c a1   .!..v0.G 7rQ%.h..
00002C55  ae b7 8e 15 b2 35 4d d0  41 6c b2 4b 0d cc df 7b   .....5M. Al.K...{
00002C65  2f 4b 6f 97 12 9c 2a 63  69 2e 32 44 ee 83 da ed   /Ko...*c i.2D....
00002C75  0e 9e f5 27 bd 3f 3e 76  b4 b0 2f 3c 98 86 2a 7a   ...'.?>v ../<..*z
00002C85  39 a7 e0 8a a1 44 71 a5  17 de f8 47 c0 c0 1d a2   9....Dq. ...G....
00002C95  60 bc 1d 90 38 ca 07 fe  5b a4 f3 c3 d9 5c 2e a2   `...8... [....\..
00002CA5  44 ce 45 77 60 8c 4f a2  69 e3 70 12 8f fa f1 68   D.Ew`.O. i.p....h
00002CB5  71 a6 3b 34 e5 8a f6 5c  0b ed 90 3a ea 81 a7 3c   q.;4...\ ...:...<
00002CC5  7c 1c 1b d9 74 00 f0 37  f0 9d 05 c0 34 09 68 6a   |...t..7 ....4.hj
00002CD5  ea 2e 22 25 1d fa c8 1e  e8 04 54 0f 58 08 14 cd   .."%.... ..T.X...
00002CE5  1c 17 14 81 e5 9a 01 d2  ed 81 75 a2 2f f3 7c dd   ........ ..u./.|.
00002CF5  50 13 f9 49 a3 b1 f6 38  6c a9 63 fd               P..I...8 l.c.
00002D01  20 c1 00 00 00 f6 01 5a  a4 29 4c d8 00 07 ec 00    ......Z .)L.....
00002D11  44 85 16 2c d1 10 71 32  f9 0f d4 54 e8 04 e6 02   D..,..q2 ...T....
00002D21  2c 89 01 1b 63 75 fc 98  99 fb 3b b0 c8 22 00 9f   ,...cu.. ..;.."..
00002D31  ff 85 ed 04 36 0b f2 47  6b b2 18 76 8a 3f ba eb   ....6..G k..v.?..
00002D41  bb 64 c0 9d 0b ab 48 c6  51 1c 8e 11 8a 7d ac a8   .d....H. Q....}..
00002D51  3f 2c db 74 19 3e 89 5e  33 06 87 36 97 d4 34 1d   ?,.t.>.^ 3..6..4.
00002D61  77 c2 3d 12 87 bf ed 5a  1e 5e b1 c9 2b 06 a4 ed   w.=....Z .^..+...
00002D71  ed 48 0d 4a 9b b7 31 85  cf 88 3b 47 38 4f 64 02   .H.J..1. ..;G8Od.
00002D81  9b ea 38 bb 60 b1 78 9b  fa 0b f5 e1 d7 1b 59 3a   ..8.`.x. ......Y:
00002D91  ab 30 74 03 03 e3 1c 29  b6 9d f7 0f c1 ed 22 f4   .0t....) ......".
00002DA1  ea b5 68 7c f4 9e f5 91  6a 08 7a ee 11 c4 1c 39   ..h|.... j.z....9
00002DB1  ea 6d 86 33 b7 64 f0 0f  cc 5f 3c 86 83 9b 7c df   .m.3.d.. ._<...|.
00002DC1  7b 06 2f d3 b5 50 f9 78  b1 d1 98 c2 84 79 46 16   {./..P.x .....yF.
00002DD1  1c 56 2e fc b2 10 bf a1  3e 89 62 10 db a6 77 6d   .V...... >.b...wm
00002DE1  0b b8 47 1c 86 fb 3d fa  05 65 ce 0e e1 e6 c2 a9   ..G...=. .e......
00002DF1  08 71 36 55 ed e7 43 7b  f0 f7 19 fd               .q6U..C{ ....
00002DFD  20 c2 00 00 00 f6 01 5a  a4 29 38 d9 00 07 ec 00    ......Z .)8.....
00002E0D  9e cf 9e ef b8 a1 ce dc  e6 f3 2e 9b cf 82 25 7f   ........ ......%.
00002E1D  be 52 c9 17 4e bd ae 0a  89 80 79 d5 78 30 d2 4f   .R..N... ..y.x0.O
00002E2D  a1 02 a6 c0 6b 3a 42 a6  23 ff 73 61 15 39 73 c3   ....k:B. #.sa.9s.
00002E3D  d1 e0 3e 8d e5 bb 5a 29  5c f8 81 f9 91 f3 ea d2   ..>...Z) \.......
00002E4D  c5 5a 4c f2 c5 d9 85 63  af a9 b6 5a c0 d1 ec 9e   .ZL....c ...Z....
00002E5D  41 14 48 c0 d0 c9 0b 8b  02 d2 dc 20 c5 f3 98 4d   A.H..... ... ...M
00002E6D  d4 8a 4f 58 41 05 02 04  72 b6 44 37 41 fa 01 15   ..OXA... r.D7A...
00002E7D  0d 2f 92 a3 22 39 5f e8  bd 22 92 78 d5 d0 3a 1d   ./.."9_. .".x..:.
00002E8D  6d d0 93 4e 74 15 e2 e9  0d 23 bc 26 ec 17 df 31   m..Nt... .#.&...1
00002E9D  41 c7 c3 58 35 98 8b 11  85 ae 65 b3 f7 47 a7 1c   A..X5... ..e..G..
00002EAD  47 42 35 03 09 72 c9 24  c8 f9 48 10 99 29 98 a3   GB5..r.$ ..H..)..
00002EBD  61 e4 e7 44 02 36 ee 03  17 2c 9c af 2d ce 61 78   a..D.6.. .,..-.ax
00002ECD  a3 d6 f7 1c 2e 4b f5 46  be d5 9b 6b 61 30 3f 73   .....K.F ...ka0?s
00002EDD  50 2e b4 fa 7c e2 15 86  d9 ec 03 2b 4f 7c 01 cd   P...|... ...+O|..
00002EED  0d 96 f1 ec 7f bd 06 15  79 11 7c f9               ........ y.|.
00002EF9  20 c3 00 00 00 f6 01 5a  a4 29 24 da 00 07 ec 00    ......Z .)$.....
00002F09  cd dc 3a 47 22 cf 12 8f  2c 74 99 ba 30 2f 10 2f   ..:G"... ,t..0/./
00002F19  f1 4c c2 5c 5b b2 b2 c0  c0 7a e1 19 51 eb a9 01   .L.\[... .z..Q...
00002F29  74 d1 5b ec 0f d1 39 2e  63 2f e9 6b be 55 15 61   t.[...9. c/.k.U.a
00002F39  f0 09 d4 54 4b 0c 37 4a  0d e6 5a 74 6e bd ce fc   ...TK.7J ..Ztn...
```



```
00002F39  f0 09 d4 54 4b 0c 37 4a  0d e6 5a 74 6e bd ce fc   ...TK.7J ..Ztn...
00002F49  10 38 a8 29 17 9d 38 f4  74 70 ca c2 a3 a6 21 62   .8.)..8. tp....!b
00002F59  9c 93 f1 00 5b 1a 6c 6c  78 27 d5 21 4a 7d 78 06   ....[.ll x'..!J}x.
00002F69  bf 70 2f f7 01 8b f6 29  4b 9e cf 3c 7f ea a9 30   .p/....) K..<...0
00002F79  ad 1c 8d 55 e3 e7 64 ea  7a ce c4 9a 5a a0 50 b7   ...U..d. z...Z.P.
00002F89  16 b4 78 f4 7a 2f 4e 4d  f7 43 32 fe cc 75 82 d7   ..x.z/NM .C2..u..
00002F99  d9 7a b6 b0 31 2d a1 b8  a9 b6 b5 08 9f 1c 73 83   .z..1-.. ......s.
00002FA9  ae 4f 2c df 49 94 ba 2d  d2 04 c4 4a 02 62 87 99   .O,.I..- ...J.b..
00002FB9  29 e5 2e 35 5f b3 e3 1e  fa 7f cb 17 17 17 72 ad   )..5_... ......r.
00002FC9  46 16 de ff c4 71 d0 21  27 1e 26 a9 3e f5 3e e7   F....q.! '.&.>.>.
00002FD9  c3 5c 17 60 d6 06 fd f1  68 d0 4d 73 b5 37 87 bf   .\.`.... h.Ms.7..
00002FE9  10 03 66 45 81 77 43 fa  03 82 41 c3               ..fE.wC. ..A.
00002FF5  20 c4 00 00 00 f6 01 5a  a4 29 10 db 00 07 ec 00    ......Z .)......
00003005  ce 3d ae 30 9f 13 f0 5b  86 e4 4c 86 5f b8 06 79   .=.0...[ ..L._..y
00003015  a6 c0 0f 5c c6 25 67 55  f8 35 1c 80 1b dc 05 4b   ...\.%gU .5.....K
00003025  4c 30 a6 45 ce 6a 3f e4  a3 a8 21 a0 08 49 49 0b   L0.E.j?. ..!..II.
00003035  9b ad a0 4e 9c dc af c2  ae 08 27 7a 11 e3 b7 a4   ...N.... ..'z....
00003045  f0 cc c5 a3 69 48 5b 22  33 36 5f 62 b4 10 55 1a   ....iH[" 36_b..U.
00003055  b5 e6 5e 4e fc 92 48 8c  d2 17 d5 b1 37 a8 65 87   ..^N..H. ....7.e.
00003065  e0 17 f4 ab b5 08 16 bb  6b 69 ab 68 d9 3d 27 4c   ........ ki.h.='L
00003075  45 00 b3 39 18 8c 9f f4  91 d1 19 f4 33 22 7d 71   E..9.... ....3"}q
00003085  1c 3f 3e f6 f1 3d b7 73  42 ad 0a 85 bc 77 1c 52   .?>..=.s B....w.R
00003095  34 6b cc 35 d1 81 28 0b  6f 4d 80 b7 fd 2c 1d 87   4k.5..(. oM...,..
000030A5  b7 6d b9 8b 15 ce f3 13  d1 92 33 c9 f3 b9 dc e7   .m...... ..3.....
000030B5  15 dd ba 10 b8 5c 3c 70  f9 9f ff 5b 08 70 91 d2   .....\<p ...[.p..
000030C5  68 77 07 e9 f1 86 56 94  6e e7 71 0d b8 f6 83 c2   hw....V. n.q.....
000030D5  7c 9b 6d 77 c7 c2 65 c8  e9 dc 01 e3 83 36 d9 b5   |.mw..e. .....6..
000030E5  fc d9 82 61 c0 71 b3 26  59 9e 6a b9               ...a.q.& Y.j.
000030F1  20 c5 00 00 00 f6 01 5a  a4 29 fc db 00 07 ec 00    ......Z .)......
00003101  12 90 39 ee 49 da e0 b1  0f 26 39 63 ff d0 17 cf   ..9.I... .&9c....
00003111  99 07 7e 68 a7 5c e8 96  00 5d bc e2 84 e9 5a 08   ..~h.\.. .]....Z.
00003121  56 2e 06 6c 41 02 a4 88  1c 1d cc 7d 30 34 b5 2f   V..lA... ...}04./
00003131  9a 8d 71 7b 13 a6 77 72  f7 05 4d ff 76 ee c3 be   ..q{..wr ..M.v...
00003141  ff 13 7a 08 67 20 4d 0b  ef 87 8b 4e f8 e4 66 5d   ..z.g M. ...N..f]
00003151  1f 24 4e 3e 97 6b 98 18  78 8e 53 05 a5 42 7e 22   .$N>.k.. x.S..B~"
00003161  72 b4 38 f5 dc e0 57 18  6c ce 45 b3 24 74 ee 7e   r.8...W. l.E.$t.~
00003171  cd 43 32 f8 ab 2c 91 6a  cf b2 cd 35 5b 36 59 b0   .C2..,.j ...5[6Y.
00003181  11 2f 48 3a 33 a4 1d 66  48 85 30 43 16 31 a3 d3   ./H:3..f H.0C.1..
00003191  3f 91 19 7c 91 21 8d 13  5b 42 72 0a 37 e4 1d 6e   ?..|.!.. [Br.7..n
000031A1  c8 85 70 43 e4 1c 74 86  52 6a ec a5 0d 3a af 33   ..pC..t. Rj...:.3
000031B1  5c 07 5d 54 f5 a2 d9 bc  d0 b4 8b 56 eb 86 63 56   \.]T.... ...V..cV
000031C1  00 25 bf 8c 71 2b 55 28  e1 8f 15 a6 80 94 aa 90   .%..q+U( ........
000031D1  08 b9 5c 22 8a 52 4c 22  5f c2 78 6c f6 f5 b1 24   ..\".RL" _.xl...$
000031E1  a6 c0 08 5e 7e b4 99 0f  58 3e 83 3f               ...^~... X>.?
000031ED  20 c6 00 00 00 f6 01 5a  a4 29 e8 dc 00 07 ec 00    ......Z .)......
000031FD  e9 7d 7e 4f 47 ed 1d 1d  f5 e2 3b a3 9e 4a 87 5c   .}~OG... ..;..J.\
0000320D  2a 1d 45 f5 87 c8 d3 b8  87 d9 c9 b3 fa 5b 4a 87   *.E..... .....[J.
0000321D  dc c3 84 64 05 b3 fd 44  b9 6a bc a3 e3 aa f8 fe   ...d...D .j......
0000322D  b8 4a a7 43 2e 93 8e a2  fa e3 3a 65 d2 de e9 e9   .J.C.... ..:e....
0000323D  69 6a 9b fb 17 e0 a4 d2  57 96 60 cf 96 db 13 76   ij...... W.`....v
0000324D  74 01 ff f9 7f 1e 39 e3  3a bb c6 1f cc eb d9 55   t.....9. :......U
0000325D  45 fe 87 fe 54 29 86 0c  be 6c 8f e9 15 36 09 0a   E...T).. .l...6..
0000326D  c6 2f 09 f1 4b 45 e2 97  ca c0 2f 0b f1 cb 45 e2   ./..KE.. ../...E.
0000327D  97 cb c0 af 08 f1 2b 45  e2 57 ca c0 5f 15 e2 af   ......+E .W.._...
0000328D  16 89 bf 5a 06 fe 9a 10  7f ad 48 fc b5 32 f0 d7   ...Z.... ..H..2..
0000329D  85 f8 eb 45 e2 af 97 81  bf 21 c4 df 28 12 7f a3   ...E.... .!..(...
000032AD  0c fc 22 73 dc 6f f2 ec  2d 23 8d 00 f8 07 3c 23   .."s.o.. -#....<#
000032BD  fb 2d 4e cf 9a 01 35 e4  85 31 3b de 77 38 49 9e   .-N...5. .1;.w8I.
```



```
000032CD  70 e4 84 2f b2 c2 a3 b1  d6 52 7f 4b 06 0f f7 49   p../.... .R.K...I
000032DD  3b b0 f9 b6 ce 1b 3e 51  e2 b3 7e 60               ;.....>Q ..~`
000032E9  20 c7 00 00 00 f6 01 5a  a4 29 d4 dd 00 07 ec 00    ......Z .)......
000032F9  72 53 6b 91 af 7d d2 02  27 23 8e 7d 32 f6 99 9c   rSk..}.. '#.}2...
00003309  f5 7f 92 78 54 a5 e7 d8  13 fa 96 93 f5 b5 8a 18   ...xT... ........
00003319  bb a1 6b a7 62 af 54 0c  83 ac cf af cd 05 52 12   ..k.b.T. ......R.
00003329  83 7c 78 e8 f5 4e 45 89  ef de 80 f0 04 2e f7 d3   .|x..NE. ........
00003339  16 96 0d a2 92 13 ae 2c  86 db eb b5 5a a7 c2 c5   ......., ....Z...
00003349  77 6f c8 02 4a 67 1c ef  84 be e5 04 ab 88 c1 6a   wo..Jg.. .......j
00003359  da 6f 27 4b 2f be 0b a5  f0 60 e0 be 71 b8 6f 8c   .o'K/... .`..q.o.
00003369  e6 0c 2f d7 44 b6 b2 6b  a4 f8 5a e3 fd c8 54 98   ../.D..k ..Z...T.
00003379  4e 35 a5 d6 1c 17 db 1d  77 27 54 e1 3b 4b 1e 8a   N5...... w'T.;K..
00003389  00 5a 7e b8 21 85 49 73  4d 48 81 5c 1e 05 28 eb   .Z~.!.Is MH.\..(.
00003399  e4 a1 50 51 af 0b 69 51  ca a3 05 07 02 aa c0 c2   ..PQ..iQ ........
000033A9  c6 41 43 48 49 b5 3c 4a  70 94 10 ad d8 41 72 95   .ACHI.<J p....Ar.
000033B9  16 d0 1d 0f 04 d9 4d d1  8a 3c ae 5b 4f 18 79 b5   ......M. .<.[O.y.
000033C9  be f0 dd b9 b8 bb 05 69  e4 f4 21 0d 37 64 14 d8   .......i ..!.7d..
000033D9  97 06 52 13 ee 1b c4 c4  ca 73 7e 4d               ..R..... .s~M
000033E5  20 c8 00 00 00 f6 01 5a  a4 29 c0 de 00 07 ec 00    ......Z .)......
000033F5  e1 09 67 ea af b6 33 bc  09 5f 63 38 27 fc 01 5c   ..g...3. ._c8'..\
00003405  87 02 5a cf c9 90 33 ca  09 7c ba f5 ee 8c ba 93   ..Z...3. .|......
00003415  03 ef e6 64 8a c8 4c ab  ad ff 7a 34 c6 e2 54 d4   ...d..L. ..z4..T.
00003425  4d 48 7e e5 84 89 8d c0  8d ab 30 73 d4 77 08 9d   MH~..... ..0s.w..
00003435  fc 8e b9 b3 66 e0 ba e8  28 61 aa ea 05 e6 37 ec   ....f... (a....7.
00003445  6c d7 a2 f3 15 32 76 bd  6b 0b 13 48 b6 d2 52 63   l....2v. k..H..Rc
00003455  19 82 3a 2f c8 66 41 77  93 9f 8d 29 5b 98 b6 f2   ..:/.fAw ...)[...
00003465  bd 91 9c a1 9a 71 ed 5c  38 e9 1b 3f a4 24 d0 6c   .....q.\ 8..?.$.l
00003475  bc c6 f5 3e 86 70 b9 88  cb cc 59 85 f4 9d b0 e0   ...>.p.. ..Y.....
00003485  1c a6 ac b8 fd 82 27 d6  93 ce f0 1c a6 80 ad 07   ......'. ........
00003495  6d 88 46 62 88 69 0d cc  f3 ce 61 5a 85 ab ae 7b   m.Fb.i.. ..aZ...{
000034A5  85 55 d2 b1 c3 84 cb 25  75 e9 02 64 c1 85 d2 1a   .U.....% u..d....
000034B5  69 5b b8 47 ae c3 9f 5e  ae 9f ae 6f 6f 70 e1 a9   i[.G...^ ...oop..
000034C5  12 6d 18 7e 39 fd a3 ba  70 6a f9 ab f6 20 a5 f0   .m.~9... pj... ..
000034D5  69 2d 34 fc e1 2d 1e 85  d9 50 8e 3d               i-4..-.. .P.=
000034E1  20 c9 00 00 00 f6 01 5a  a4 29 ac df 00 07 ec 00    ......Z .)......
000034F1  c7 3c ae fd a5 b2 9c a0  ab 29 a0 e5 63 40 cb df   .<...... .)..c@..
00003501  08 74 2d 05 b4 72 0c 68  65 5b 1a 11 e3 f6 e6 a7   .t-..r.h e[......
00003511  48 11 7b 65 52 23 32 27  98 9a d2 69 65 51 34 7c   H.{eR#2' ...ieQ4|
00003521  35 e9 d5 32 77 b6 c4 23  49 9d d6 05 c1 30 e4 c2   5..2w..# I....0..
00003531  e1 39 f0 a8 4c b8 8e 39  27 e1 f2 6b 94 e1 d5 93   .9..L..9 '..k....
00003541  65 89 74 79 0d 5b 89 2e  5a 58 03 f1 51 a5 e4 cc   e.ty.[.. ZX..Q...
00003551  57 c9 b2 74 28 67 51 23  0b cb 74 1d 2f 74 b0 d6   W..t(gQ# ..t./t..
00003561  53 ce 23 97 14 c5 0b 46  61 22 34 5f 4e 8c 33 cc   S.#....F a"4_N.3.
00003571  c2 95 a3 a8 bc 98 85 c5  46 86 85 c5 a2 19 92 61   ........ F......a
00003581  c1 f1 c0 ac 37 23 b7 a4  04 6e 15 b2 f2 d8 c8 b0   ....7#.. .n......
00003591  f2 58 20 b7 4e 5d 91 cc  c8 2a 39 81 55 85 2c 4b   .X .N].. .*9.U.,K
000035A1  36 44 0a 52 1b 3e 76 07  6a 2b 8d 53 e0 77 e0 74   6D.R.>v. j+.S.w.t
000035B1  8c 86 9e 06 d8 4e 13 4c  27 3a 1f 73 87 4e 72 c2   .....N.L ':.s.Nr.
000035C1  13 27 e3 3d f6 c7 2d c1  d2 50 cb 59 d9 a0 97 c2   .'.=..-. .P.Y....
000035D1  bc 06 e9 7c 67 1f 8f 65  4f c0 05 9d               ...|g..e O...
000035DD  20 ca 00 00 00 f6 01 5a  a4 29 98 e0 00 07 ec 00    ......Z .)......
000035ED  04 3c 75 35 da 43 e5 f1  3c 4e 8c f5 80 d3 bc c8   .<u5.C.. <N......
000035FD  a9 ac 1b 8d 54 e8 72 46  e8 f2 b7 86 7e 95 0a 5d   ....T.rF ....~..]
0000360D  c9 08 5d f9 d6 d0 af 53  a1 57 33 42 af 7e 63 e8   ..]....S .W3B.~c.
0000361D  57 22 ab a7 f6 d5 b4 7c  2b 9d 9a b3 9d 0d a7 71   W".....| +......q
0000362D  e6 55 ac b8 16 2f 6c 32  e1 a7 20 50 b0 ff e1 f4   .U.../l2 .. P....
0000363D  2a 27 e6 6b 91 53 68 74  ee fb 00 79 a4 67 74 4a   *'.k.Sht ...y.gtJ
0000364D  3c eb d5 c6 3d b1 e0 10  86 7b 49 78 cc c7 8c 0e   <...=... .{Ix....
0000365D  a1 c2 44 ed 65 e8 f1 a3  f2 0d 9f 38 e7 c9 cb cc   ..D.e... ...8....
```



```
0000366D  5d 70 2a 77 f3 9d 9d 75  86 33 df b3 2a da de 93   ]p*w...u .3..*...
0000367D  91 d8 5a 16 62 a5 7f 17  6a 85 e9 05 ea 93 9e ba   ..Z.b... j.......
0000368D  f9 ea 5d 8e 28 5a 2f f8  bb 44 7f d8 a2 af b6 e3   ..].(Z/. .D......
0000369D  f9 96 e9 71 ff 18 b7 60  5d c6 7b b2 a6 51 f0 8f   ...q...` ].{..Q..
000036AD  33 62 8b 0b 71 c2 7a 69  d9 80 d7 22 c5 67 74 a5   3b..q.zi ...".gt.
000036BD  e1 00 a3 1c c9 14 0f 1d  ef dd 41 08 eb 31 b8 b3   ........ ..A..1..
000036CD  4b 08 27 e2 2c 9c e5 63  48 c2 8b b7               K.'.,..c H...
000036D9  20 cb 00 00 00 f6 01 5a  a4 29 84 e1 00 07 ec 00    .......Z .)......
000036E9  05 f2 2c 49 be 3e fe be  2a 7e 4a 20 b2 03 43 17   ..,I.>.. *~J ..C.
000036F9  8e 1b 3e 16 cf 61 73 12  7e 2d 24 5c 2e 8c 70 f9   ..>..as. ~-$\..p.
00003709  2f 46 b8 54 a9 88 23 16  b9 28 5f cf 0f 71 7b db   /F.T..#. .(_..q{.
00003719  5f 8e 72 49 2c ec a9 c9  5c d1 57 74 b9 d3 c7 77   _.rI,... \.Wt...w
00003729  f4 9d 87 b4 84 a1 24 dc  e9 b7 d9 07 05 f7 de 9c   ......$. ........
00003739  80 6f 15 8c 0f ae c3 99  a4 33 79 01 4e 45 e9 2e   .o...... .3y.NE..
00003749  79 e9 91 c5 32 7c 34 3d  f2 9f 4c 8f 22 ee 1f dc   y...2|4= ..L."...
00003759  4e 22 36 36 5b 82 84 c2  13 85 5a f9 5e 9f bd 0d   N"66[... ..Z.^...
00003769  80 71 0f ee 12 ac 94 98  77 5d a9 8a 7b ab 04 ea   .q...... w]..{...
00003779  e4 5d ea aa 65 52 57 4b  ef 3b f9 5f b7 ef ea e9   .]..eRWK .;._....
00003789  7d 27 ff eb f6 5d 43 18  6b d1 d4 56 4a 36 22 3c   }'...]C. k..VJ6"<
00003799  b3 95 c1 77 d3 6c de 68  da 4d ab 75 a3 eb 37 ed   ...w.l.h .M.u..7.
000037A9  76 b8 e3 b9 c1 b3 f6 6e  0a cc 3e 94 2a 57 69 b0   v......n ..>.*Wi.
000037B9  e5 dc b0 af 78 fa 21 14  16 b7 cd a4 72 9d 06 5b   ....x.!. ....r..[
000037C9  29 04 76 78 79 a6 14 04  5b b8 81 ca               ).vxy... [...
000037D5  20 cc 00 00 00 f6 01 5a  a4 29 70 e2 00 07 ec 00    .......Z .)p.....
000037E5  d0 1e 3e e9 7d b5 d9 15  38 c7 ba 1d 9e 4e c1 7d   ..>.}... 8....N.}
000037F5  61 2f fa bd 5e d4 c1 a8  92 39 63 93 60 0e 1e 03   a/..^... .9c.`...
00003805  1e af eb 6d 9f f3 b2 76  84 f1 34 50 fe 4e 58 4b   ...m...v ..4P.NXK
00003815  f8 31 9c 7c 74 5d a5 84  98 47 83 6e 67 20 3c 8e   .1.|t].. .G.ng <.
00003825  37 0c 0a 75 06 04 4d e1  ce 0a 25 77 8b 4a dc 25   7..u..M. ..%w.J.%
00003835  28 12 a5 ce 60 30 1c 0b  77 5a 85 b8 1d be 1d 1b   (...`0.. wZ......
00003845  dc 55 f6 75 49 6d be c9  6a e1 f0 7e d8 f5 cc ca   .U.uIm.. j..~....
00003855  23 43 ae 08 c9 48 3d e6  25 da 37 11 a3 c7 7d e7   #C...H=. %.7...}.
00003865  11 05 a5 f7 80 2c a5 9b  3d 25 97 61 98 a2 ef 0b   .....,.. =%.a....
00003875  73 e7 3f d8 9f 61 f8 64  39 dd f0 15 4e df 37 34   s.?..a.d 9...N.74
00003885  7d b2 70 f4 ab 23 29 9b  f0 c5 9b 84 03 6f b3 54   }.p..#). .....o.T
00003895  86 65 1a 75 7d d7 c2 15  69 a9 4c 22 ae c5 44 c8   .e.u}... i.L"..D.
000038A5  45 11 21 97 48 84 70 f7  9c fe ab 2e f5 3a da 68   E.!.H.p. .....:.h
000038B5  90 89 88 f0 a0 60 41 f6  65 98 67 f1 7d a7 72 21   .....`A. e.g.}.r!
000038C5  47 89 f8 79 c1 4b 62 f0  72 29 e0 95               G..y.Kb. r)..
000038D1  20 cd 00 00 00 f6 01 5a  a4 29 5c e3 00 07 ec 00    .......Z .)\.....
000038E1  82 c0 cb 62 f0 4a 29 e0  ab 05 81 17 67 16 e8 d5   ...b.J). ....g...
000038F1  52 c0 d7 0a 02 2f ce 30  d0 6b 05 82 1f cf c0 61   R..../.0 .k.....a
00003901  9c e1 52 5c 05 6f 3c 18  5a a5 20 22 c4 19 07 7a   ..R\.o<. Z. "...z
00003911  bd 14 22 a4 82 89 a8 8b  89 68 94 da 13 52 41 44   .."..... .h...RAD
00003921  34 c4 44 5c 95 da 13 45  11 21 b2 c8 43 7d 84 d9   4.D\...E .!..C}..
00003931  10 39 29 38 b4 13 2b 2f  6a 91 09 c6 f3 47 47 83   .9)8..+/ j....GG.
00003941  4c a8 31 0c 10 7e 9c 28  ca bc d9 84 56 a3 33 fa   L.1..~.( ....V.3.
00003951  c3 c9 51 de c3 30 c4 5b  05 80 cd 02 29 09 3f 9b   ..Q..0.[ ....).?.
00003961  c4 bd 35 3c 94 c1 f3 51  1e 36 a7 0f 9e c5 07 8e   ..5<...Q .6......
00003971  48 e7 a2 c3 f0 b2 22 bd  4e 73 0b 4a 71 09 f2 2e   H.....". Ns.Jq...
00003981  6d 4a b5 4a 9a 47 50 8a  37 90 1f b7 94 e6 0c 94   mJ.J.GP. 7.......
00003991  e2 08 e4 c7 2d a7 f9 01  a5 f8 00 f9 71 2b 69 2e   ....-... ....q+i.
000039A1  40 31 b8 fd c3 e6 3f 3f  fe 6a 9a f5 2f 1a bf 54   @1....?? .j../..T
000039B1  2c fe 5a 9a e1 2f 8b ff  52 31 f8 eb 69 36 bf 2c   ,.Z../.. R1..i6.,
000039C1  fe 17 84 bf 91 6e ee 73  93 00 f5 74               .....n.s ...t
000039CD  20 ce 00 00 00 f6 01 5a  a4 29 48 e4 00 07 ec 00    .......Z .)H.....
000039DD  06 ad 8e b6 36 f8 f9 61  a7 78 29 ea d3 7d 36 d4   ....6..a .x)..}6.
000039ED  09 9b 05 77 f7 05 96 48  87 d0 bc 3e 55 8a a7 63   ...w...H ...>U..c
```

```
000039FD  6b ff 78 6e f4 75 f1 8e  77 a9 2c f4 c5 88 7e 5d   k.xn.u.. w.,...~]
00003A0D  bc df 5d 2e 0b 7d 31 0e  8e 78 e3 c3 93 52 16 fa   ..]..}1. .x...R..
00003A1D  62 dc 1c f1 86 84 a7 6a  59 e8 8b 71 76 c4 3b 13   b......j Y..qv.;.
00003A2D  9e 6a 65 a1 2f c6 e5 11  6f 51 78 aa 97 85 be 5e   .je./... oQx....^
00003A3D  0c 7a f1 2e f7 46 59 e8  1b c5 a0 17 2e f5 0e 5a   .z...FY. .......Z
00003A4D  e9 47 dc 79 a6 6b bd c4  df 67 b2 bd 55 38 13 e4   .G.y.k.. .g..U8..
00003A5D  b9 e3 78 3a 71 bc 65 82  53 81 c7 17 c7 79 70 79   ..x:q.e. S....ypy
00003A6D  81 a7 6c 6e 1f 3f 68 e9  4b 5d 08 cc 5e cf 5e d7   ..ln.?h. K]..^.^.
00003A7D  b9 4a 51 12 cb 58 1b 12  8f b9 5f f8 e6 10 db 0e   .JQ..X.. .._.....
00003A8D  a7 e1 5e b8 51 3f e7 fe  0e 49 b8 c1 a3 df 34 ba   ..^.Q?.. .I....4.
00003A9D  52 7b a4 f6 74 e1 09 ab  81 ed ef 93 c0 17 4f a0   R{..t... ......O.
00003AAD  d0 85 9e 58 58 be bf f9  3a 46 a6 13 ba b3 82 97   ...XX... :F......
00003ABD  52 c0 cb 25 82 97 f3 82  97 85 e0 1f               R..%.... ....
00003AC9  20 cf 00 00 00 f6 01 5a  a4 29 34 e5 00 07 ec 00    .......Z .)4.....
00003AD9  8d 66 c1 e0 a1 46 9e 21  65 b3 79 5e e8 8a 10 3a   .f...F.! e.y^...:
00003AE9  c8 6b 81 d0 b7 06 01 a8  a2 78 6c e4 a5 a0 9a 26   .k...... .xl....&
00003AF9  f6 83 9f 4f 43 bf f9 ca  2d fc c7 ac 2f 25 49 7e   ...OC... -.../%I~
00003B09  2d 4d f2 cb c5 9f 5b f8  eb 69 c2 5f 3c fe 02 e5   -M....[. .i._<...
00003B19  bf 91 26 ff c5 a2 2f 67  08 5c a5 0d 81 d4 0d 99   ..&.../g .\......
00003B29  c9 74 ac d1 5b 71 bc b8  8c 41 70 9d 36 08 ca a6   .t..[q.. .Ap.6...
00003B39  20 ef 30 b8 aa a4 0d 83  32 28 28 6e 20 5c 49 69    .0..... 2((n \Ii
00003B49  03 a1 68 fc a5 0c 85 2b  91 29 6e 19 c3 94 93 d9   ..h....+ .)n.....
00003B59  47 50 b3 cf c8 bd 4b 97  33 cb 5c 7f f0 60 e3 ab   GP....K. 3.\..`..
00003B69  85 e7 b4 e7 05 a9 88 41  a6 70 3a 01 64 18 9c da   .......A .p:.d...
00003B79  f9 f0 7a 5e 9c 22 d3 da  c2 ef e9 fe 9a 71 a3 4a   ..z^.".. .....q.J
00003B89  8c 11 bf 60 41 f8 8b 7c  d7 e5 d6 67 54 66 8e 83   ...`A..| ...gTf..
00003B99  1f 9a b2 89 83 82 20 fc  d4 45 56 f4 35 31 97 8f   ...... . .EV.51..
00003BA9  3b 25 7c ef 70 f0 c3 7d  90 17 b1 38 db 74 38 1e   ;%|.p..} ...8.t8.
00003BB9  15 ec 47 46 43 70 41 97  4b fe 61 a1               ..GFCpA. K.a.
00003BC5  20 d0 00 00 00 f6 01 5a  a4 29 20 e6 00 07 ec 00    .......Z .) .....
00003BD5  fc bb cc a5 2b 71 ea e9  70 a4 6b 79 88 48 f6 09   ....+q.. p.ky.H..
00003BE5  4a a0 e5 5a ac d3 3b d0  21 aa 94 bf 33 b6 b4 1f   J..Z..;. !...3...
00003BF5  1e 95 51 dc c1 e6 52 3a  7c b9 78 f8 32 0c ec 42   ..Q...R: |.x.2..B
00003C05  e0 cb 29 f0 41 94 a4 9c  f6 a8 34 d6 2b e9 d8 e5   ..).A... ..4.+...
00003C15  82 b1 17 c6 f7 6a 0a f6  4f 8f 9a d6 fb 04 43 f8   .....j.. O.....C.
00003C25  58 ee 07 76 64 48 01 3d  90 e2 d1 d7 6f d2 17 b5   X..vdH.= ....o...
00003C35  ac f4 c8 a5 d2 53 58 ff  d4 33 d1 d3 e9 3f 1d db   .....SX. .3...?..
00003C45  3f 56 74 86 cf 9f d4 4f  8d ac 74 c9 df 84 ae c2   ?Vt....O ..t.....
00003C55  fa eb 2a 85 2e 4d 19 e9  bf 1c db 57 26 b8 7b 1e   ..*..M.. ...W&.{.
00003C65  51 00 fe 3f 02 e6 f9 df  a2 7f ae b3 d0 21 97 46   Q..?.... .....!.F
00003C75  47 41 fd 21 57 2a a9 74  e4 18 3b df bc 5f e4 8a   GA.!W*.t ..;.._..
00003C85  94 85 1e b9 74 7a 0a eb  1f 91 dd ef 0c 3b fd 4e   ....tz.. .....;.N
00003C95  5f 94 9e 37 62 74 12 12  13 e6 d1 a8 9e c7 16 2f   _..7bt.. ......./
00003CA5  e0 30 76 6c 98 bb e1 a9  31 61 72 59 5e 94 4a 0a   .0vl.... 1arY^.J.
00003CB5  4a a3 f3 77 3d 0f 4a c3  fa 83 e5 c5               J..w=.J. ....
00003CC1  20 d1 00 00 00 f6 01 5a  a4 29 0c e7 00 07 ec 00    .......Z .)......
00003CD1  28 fe b2 c4 e0 71 9c 95  95 51 62 60 59 bc ac a5   (....q.. .Qb`Y...
00003CE1  e1 cc ca cc 44 9c 45 70  b3 2e 44 d9 6f e2 c1 93   ....D.Ep ..D.o...
00003CF1  80 f5 58 05 b8 89 2d e0  7a 9c 83 df 7f df 1d 5a   ..X...-. z......Z
00003D01  79 71 37 84 b8 db 5d f5  be d3 ea 66 62 ef f6 78   yq7...]. ...fb..x
00003D11  9f ce e9 2b f8 a4 ce 22  0c 3c e0 8e a8 25 35 3f   ...+..." .<...%5?
00003D21  33 ff 86 74 26 f8 cd 20  fe 31 b8 9f f0 bb 7c a3   3..t&..  .1....|.
00003D31  c0 8e 2f 25 b8 d4 79 8c  22 2a 90 d3 d5 05 22 db   ../%..y. "*....".
00003D41  fd 16 e4 ed fd dc 79 a1  f3 a1 8b 1b f5 7c 8b ad   ......y. .....|..
00003D51  bf 10 89 9f 26 ee 6c ce  58 f3 c8 65 7c 07 da 58   ....&.l. X..e|..X
00003D61  52 fb ed f0 4d a8 e8 77  e8 83 ed 9b 1b 36 f4 c1   R...M..w .....6..
00003D71  ed be 33 d4 b6 4e ba f4  85 f4 e8 d4 a2 b7 97 bc   ..3..N.. ........
00003D81  30 c6 9b fc 7a 5c f3 70  9d 73 bb a9 57 e5 1f c6   0...z\.p .s..W...
```

```
00003D91  bc 9b d2 39 2e fd 45 57  eb bb 43 50 bb a8 4d d7   ...9..EW ..CP..M.
00003DA1  20 91 06 6a 3f 59 6c 75  e7 bb 01 0a 73 74 b5 87    ..j?Ylu ....st..
00003DB1  e2 5d 53 b7 ea e6 b4 8f  02 70 c0 23               .]S..... .p.#
00003DBD  20 d2 00 00 00 ed 01 5a  a4 29 f8 e7 00 07 e3 00    .......Z .)......
00003DCD  82 fa 6e c3 c0 48 67 19  ed fb 67 5b 8c dc 2a dc   ..n..Hg. ..g[..*.
00003DDD  aa 2d e9 85 db 1e ae f5  ee ec ee da aa eb fd 4d   .-...... .......M
00003DED  dd f6 2d 14 85 ad aa 93  6b b8 fd 99 b1 65 18 31   ..-..... k....e.1
00003DFD  18 ae 0f ac 8c 59 70 f0  5e 28 88 07 e5 0e 06 1f   .....Yp. ^(......
00003E0D  f7 25 9b e1 9e d2 cb 48  44 99 cd 5c cb 8c cf 5c   .%.....H D..\...\
00003E1D  de bd a9 05 9e ef 2c c2  01 b7 2e 1c bb d4 64 78   ......,. ......dx
00003E2D  3e 6d 93 7a 8c 1f 54 5b  33 98 79 7b b9 5b 1e 56   >m.z..T[ 3.y{.[.V
00003E3D  ee d2 a9 c9 fc a1 13 84  6f e3 98 f1 69 8b fa 94   ........ o...i...
00003E4D  b3 e1 ed ee ff 01 50 4b  01 02 33 00 2d 00 00 00   ......PK ..3.-...
00003E5D  08 00 20 08 21 44 0f 1a  ea b4 ff ff ff ff ff ff   .. .!D.. ........
00003E6D  ff ff 05 00 14 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003E7D  00 00 00 00 65 6e 74 72  79 01 00 10 00 e0 c2 00   ....entr y.......
00003E8D  00 00 00 00 00 3c 18 00  00 00 00 00 00 50 4b 05   .....<.. ......PK.
00003E9D  06 00 00 00 00 01 00 01  00 47 00 00 00 73 18 00   ........ .G...s..
00003EAD  00 00 00                                           ...
00003EB0  20 d3 00 00 00 9e 01 5a  a4 29 6c 4f 04 07 94 00    .......Z .)lO....
00003EC0  aa aa 00 00 00 00 94 00  01 00 00 00 87 07 00 01   ........ ........
00003ED0  0a 00 00 00 78 00 00 00  00 01 00 00 d4 fe 01 00   ....x... ........
00003EE0  2c 01 00 00 01 02 00 00  00 02 00 00 ec 02 00 00   ,....... ........
00003EF0  02 06 00 00 ec 04 00 00  03 00 00 00 03 08 01 00   ........ ........
00003F00  00 80 01 07 40 00 00 00  04 08 01 00 00 81 01 07   ....@... ........
00003F10  a0 0f 00 00 05 07 01 00  a0 90 01 07 08 00 00 00   ........ ........
00003F20  06 03 01 00 6c 91 01 07  6c 01 00 00 07 04 01 00   ....l... l.......
00003F30  d8 92 01 07 a8 00 00 00  08 05 01 00 e8 e0 01 07   ........ ........
00003F40  41 03 00 00 09 09 01 00  00 d0 00 07 00 b0 00 00   A....... ........
00003F50  bd 77 00 00                                        .w..
00003F54  20 d4 00 00 00 f6 01 5a  a4 29 00 02 00 00 ec 00    .......Z .)......
00003F64  06 00 ec 02 a8 90 01 07  6c 91 01 07 b0 90 01 07   ........ l.......
00003F74  10 20 01 00 7c 91 01 07  d0 90 01 07 02 2a 01 00   . ..|... .....*..
00003F84  7e 91 01 07 fa 90 01 07  06 10 01 00 00 00 00 00   ~....... ........
00003F94  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003FA4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003FB4  84 91 01 07 0a 91 01 07  04 08 04 00 00 00 00 00   ........ ........
00003FC4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003FD4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003FE4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00003FF4  00 00 00 00 00 00 00 00  94 91 01 07 2a 91 01 07   ........ ....*...
00004004  9c 06 01 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004014  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004024  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004034  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004044  30 92 01 07 30 91 01 07  a8 3c 01 00               0...0... .<..
00004050  20 d5 00 00 00 f6 01 5a  a4 29 ec 02 00 00 ec 00    .......Z .)......
00004060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000040F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

```
00004110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004140  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
0000414C  20 d6 00 00 00 f6 01 5a  a4 29 d8 03 00 00 ec 00    .......Z .)......
0000415C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000416C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000417C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000418C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000419C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041AC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041CC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041DC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041EC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000041FC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000420C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000421C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000422C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000423C  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00004248  20 d7 00 00 00 35 01 5a  a4 29 c4 04 00 00 2b 00    ....5.Z .)....+.
00004258  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004268  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004278  00 00 00 00 00 00 00 00  03 02 02                  ........ ...
00004283  20 d8 00 00 00 f6 01 5a  a4 29 d4 fe 01 00 ec 00    .......Z .)......
00004293  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042A3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042B3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042C3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042D3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042E3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000042F3  00 00 00 00 00 00 06 01  6c 4f 04 07 94 00 00 00   ........ lO......
00004303  00 d0 00 07 db 18 00 00  ac 67 01 00 01 02 00 00   ........ .g......
00004313  00 00 00 00 00 80 01 07  40 80 01 07 00 80 01 07   ........ @.......
00004323  00 02 d0 07 00 81 01 07  00 00 00 00 00 00 02 00   ........ ........
00004333  a0 90 01 07 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00004343  00 00 a8 00 d8 92 01 07  41 03 00 00 e8 e0 01 07   ........ A.......
00004353  03 00 00 00 ec 04 00 00  ff 00 00 00 00 02 00 00   ........ ........
00004363  43 6b 02 00 68 4d 00 00  00 00 11 7b 5d 05 00 00   Ck..hM.. ...{]...
00004373  ef 02 05 00 00 00 fa 00  04 00 01 01               ........ ....
0000437F  20 d9 00 00 00 4a 01 5a  a4 29 c0 ff 01 00 40 00    ....J.Z .)....@.
0000438F  00 00 00 00 87 07 01 00  10 00 10 00 53 41 46 45   ........ ....SAFE
0000439F  20 4c 61 62 20 4d 61 66  69 61 00 00 00 00 00 00    Lab Maf ia......
000043AF  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000043BF  00 00 00 00 00 00 ec 02  2c 01 00 04 19 b1 d1 d2   ........ ,.......
```

Figure 22: Suspicious instructed uploaded by the host 192.168.10.164

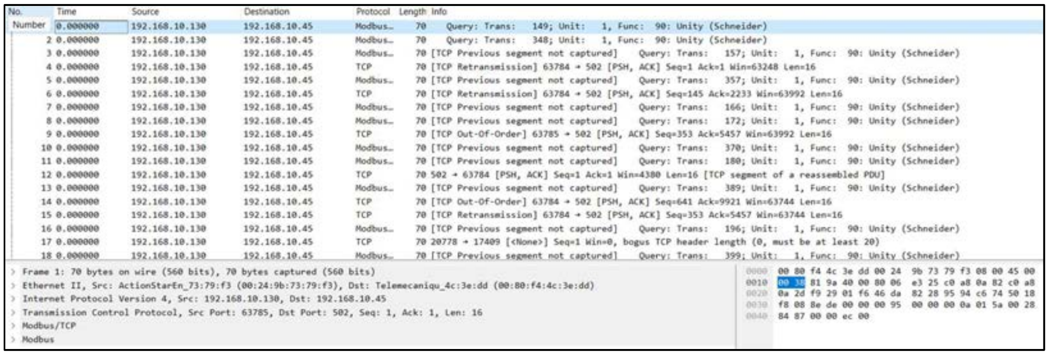
Findings:

The workstation bearing IP 192.168.10.164 writes instructions to the PLC system only.

Analysis 2:

We have used “Bulk Extractor (Kali Linux)” to all On-Chip PLC Memory dumps and extracted following “pcap” (Network Log Files) files. The "pcap" files don't have any packet timestamps, as given in figure 23. Consequently, we presume that the time for the initial packet transmission is the same as the OnChip PLC memory dump acquisition time.

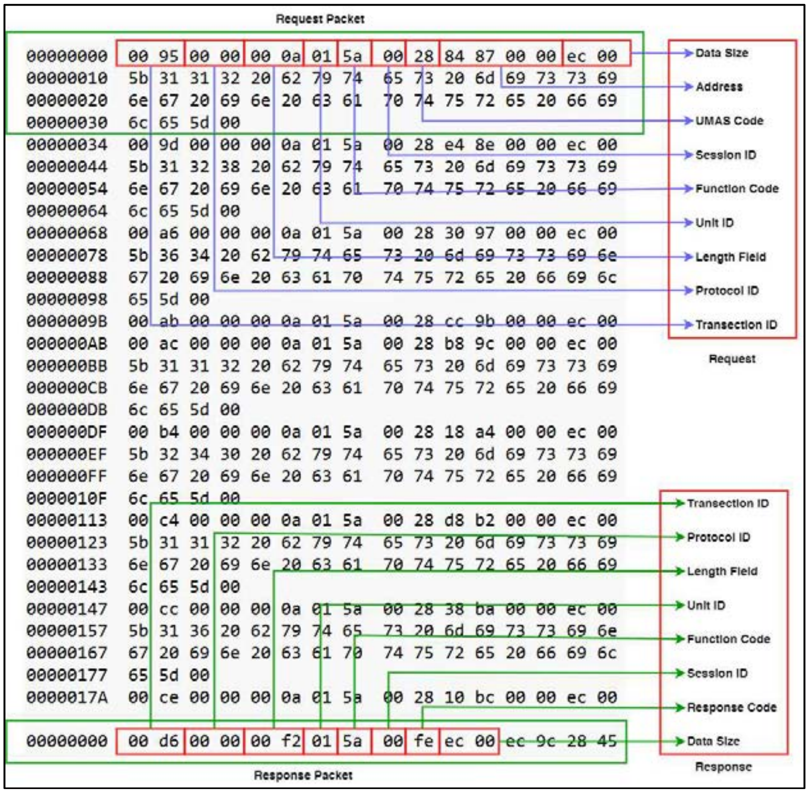
Extracted “pacap” labels	**from OnCchipRAM202306291XXXXX.bin**
PLC_NET1	43506
PLC_NET2	45007
PLC_NET3	50509
PLC_NET4	52010
PLC_NET5	53511
PLC_NET6	55012
PLC_NET7	60514



```
No.     Time      Source          Destination    Protocol Length Info
Number  0.000000  192.168.10.130  192.168.10.45  Modbus…  70     Query: Trans:   149; Unit:   1, Func:  90: Unity (Schneider)
      2 0.000000  192.168.10.130  192.168.10.45  Modbus…  70     Query: Trans:   348; Unit:   1, Func:  90: Unity (Schneider)
      3 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   157; Unit:   1, Func:  90: Unity (Schneider)
      4 0.000000  192.168.10.130  192.168.10.45  TCP      70 [TCP Retransmission] 63784 → 502 [PSH, ACK] Seq=1 Ack=1 Win=63248 Len=16
      5 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   357; Unit:   1, Func:  90: Unity (Schneider)
      6 0.000000  192.168.10.130  192.168.10.45  TCP      70 [TCP Retransmission] 63784 → 502 [PSH, ACK] Seq=145 Ack=2233 Win=63992 Len=16
      7 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   166; Unit:   1, Func:  90: Unity (Schneider)
      8 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   172; Unit:   1, Func:  90: Unity (Schneider)
      9 0.000000  192.168.10.130  192.168.10.45  TCP      70 [TCP Out-Of-Order] 63785 → 502 [PSH, ACK] Seq=353 Ack=5457 Win=63992 Len=16
     10 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   370; Unit:   1, Func:  90: Unity (Schneider)
     11 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   180; Unit:   1, Func:  90: Unity (Schneider)
     12 0.000000  192.168.10.130  192.168.10.45  TCP      70 502 → 63784 [PSH, ACK] Seq=1 Ack=1 Win=4380 Len=16 [TCP segment of a reassembled PDU]
     13 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   389; Unit:   1, Func:  90: Unity (Schneider)
     14 0.000000  192.168.10.130  192.168.10.45  TCP      70 [TCP Out-Of-Order] 63784 → 502 [PSH, ACK] Seq=641 Ack=9921 Win=63744 Len=16
     15 0.000000  192.168.10.130  192.168.10.45  TCP      70 [TCP Retransmission] 63784 → 502 [PSH, ACK] Seq=353 Ack=5457 Win=63744 Len=16
     16 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   196; Unit:   1, Func:  90: Unity (Schneider)
     17 0.000000  192.168.10.130  192.168.10.45  TCP      70 20778 → 17409 [<None>] Seq=1 Win=0, bogus TCP header length (0, must be at least 20)
     18 0.000000  192.168.10.130  192.168.10.45  Modbus…  70 [TCP Previous segment not captured]    Query: Trans:   399; Unit:   1, Func:  90: Unity (Schneider)

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: ActionStarEn_73:79:f3 (00:24:9b:73:79:f3), Dst: Telemecaniqu_4c:3e:dd (00:80:f4:4c:3e:dd)
> Internet Protocol Version 4, Src: 192.168.10.130, Dst: 192.168.10.45
> Transmission Control Protocol, Src Port: 63785, Dst Port: 502, Seq: 1, Ack: 1, Len: 16
> Modbus/TCP
> Modbus

0000  00 80 f4 4c 3e dd 00 24  9b 73 79 f3 08 00 45 00
0010  00 38 81 9a 40 00 80 06  e3 25 c0 a8 0a 82 c0 a8
0020  0a 2d f9 29 01 f6 46 da  82 28 95 94 c6 74 50 18
0030  f8 08 8e de 00 00 00 95  00 00 00 0a 01 5a 00 28
0040  84 87 00 00 ec 00
```

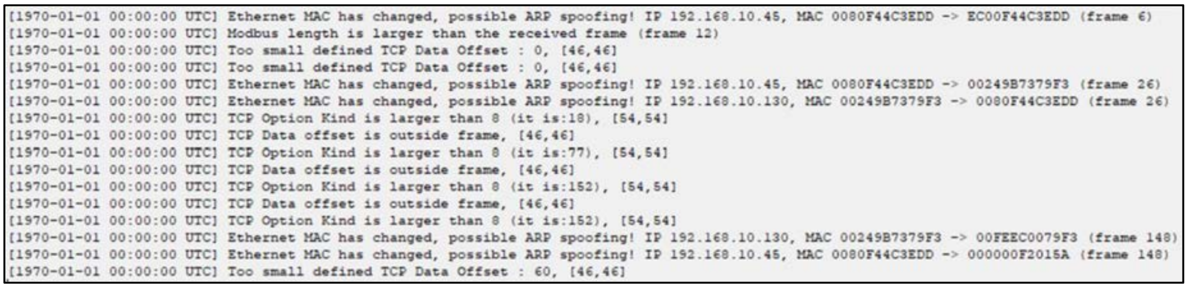
Figure 23: Erroneous packet transmission timestamp

We have analyzed each Modbus TCP packets and decipher the codes accordingly. The decoded packet sample are given in figure 24. Moreover, we identified an ARP spoofing exploitation as shown in figure 25.



```
00000000  00 95 00 00 00 0a 01 5a  00 28 84 87 00 00 ec 00
00000010  5b 31 31 32 20 62 79 74  65 73 20 6d 69 73 73 69
00000020  6e 67 20 69 6e 20 63 61  70 74 75 72 65 20 66 69
00000030  6c 65 5d 00
00000034  00 9d 00 00 00 0a 01 5a  00 28 e4 8e 00 00 ec 00
00000044  5b 31 32 38 20 62 79 74  65 73 20 6d 69 73 73 69
00000054  6e 67 20 69 6e 20 63 61  70 74 75 72 65 20 66 69
00000064  6c 65 5d 00
00000068  00 a6 00 00 00 0a 01 5a  00 28 30 97 00 00 ec 00
00000078  5b 36 34 20 62 79 74 65  73 20 6d 69 73 73 69 6e
00000088  67 20 69 6e 20 63 61 70  74 75 72 65 20 66 69 6c
00000098  65 5d 00
0000009B  00 ab 00 00 00 0a 01 5a  00 28 cc 9b 00 00 ec 00
000000AB  00 ac 00 00 00 0a 01 5a  00 28 b8 9c 00 00 ec 00
000000BB  5b 31 31 32 20 62 79 74  65 73 20 6d 69 73 73 69
000000CB  6e 67 20 69 6e 20 63 61  70 74 75 72 65 20 66 69
000000DB  6c 65 5d 00
000000DF  00 b4 00 00 00 0a 01 5a  00 28 18 a4 00 00 ec 00
000000EF  5b 32 34 30 20 62 79 74  65 73 20 6d 69 73 73 69
000000FF  6e 67 20 69 6e 20 63 61  70 74 75 72 65 20 66 69
0000010F  6c 65 5d 00
00000113  00 c4 00 00 00 0a 01 5a  00 28 d8 b2 00 00 ec 00
00000123  5b 31 31 32 20 62 79 74  65 73 20 6d 69 73 73 69
00000133  6e 67 20 69 6e 20 63 61  70 74 75 72 65 20 66 69
00000143  6c 65 5d 00
00000147  00 cc 00 00 00 0a 01 5a  00 28 38 ba 00 00 ec 00
00000157  5b 31 36 20 62 79 74 65  73 20 6d 69 73 73 69 6e
00000167  67 20 69 6e 20 63 61 70  74 75 72 65 20 66 69 6c
00000177  65 5d 00
0000017A  00 ce 00 00 00 0a 01 5a  00 28 10 bc 00 00 ec 00

00000000  00 d6 00 00 00 f2 01 5a  00 fe ec 00 ec 9c 28 45
```

Figure 24: Decoded Modbus TCP in “pcap” file



```
[1970-01-01 00:00:00 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.45, MAC 0080F44C3EDD -> EC00F44C3EDD (frame 6)
[1970-01-01 00:00:00 UTC] Modbus length is larger than the received frame (frame 12)
[1970-01-01 00:00:00 UTC] Too small defined TCP Data Offset : 0, [46,46]
[1970-01-01 00:00:00 UTC] Too small defined TCP Data Offset : 0, [46,46]
[1970-01-01 00:00:00 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.45, MAC 0080F44C3EDD -> 00249B7379F3 (frame 26)
[1970-01-01 00:00:00 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.130, MAC 00249B7379F3 -> 0080F44C3EDD (frame 26)
[1970-01-01 00:00:00 UTC] TCP Option Kind is larger than 8 (it is:18), [54,54]
[1970-01-01 00:00:00 UTC] TCP Data offset is outside frame, [46,46]
[1970-01-01 00:00:00 UTC] TCP Option Kind is larger than 8 (it is:77), [54,54]
[1970-01-01 00:00:00 UTC] TCP Data offset is outside frame, [46,46]
[1970-01-01 00:00:00 UTC] TCP Option Kind is larger than 8 (it is:152), [54,54]
[1970-01-01 00:00:00 UTC] TCP Data offset is outside frame, [46,46]
[1970-01-01 00:00:00 UTC] TCP Option Kind is larger than 8 (it is:152), [54,54]
[1970-01-01 00:00:00 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.130, MAC 00249B7379F3 -> 00FEEC0079F3 (frame 148)
[1970-01-01 00:00:00 UTC] Ethernet MAC has changed, possible ARP spoofing! IP 192.168.10.45, MAC 0080F44C3EDD -> 000000F2015A (frame 148)
[1970-01-01 00:00:00 UTC] Too small defined TCP Data Offset : 60, [46,46]
```

Figure 25: ARP spoofing of the PLC system bearing the IP 192.168.10.45

Findings:

1) Only computer that has established connectivity with the PLC system and been extracted from the "pcap" files is the "Engineering Workstation (with Logging)" with IP address 192.168.10.130.

2) All decoded Modbus TCP requests are in the form of “READ_FNC” (UMAS Code 0x28) that denotes 192.168.10.130 is not in the “suspect” list.

3) ARP spoofing is the important discovery that indicates the presence of the malware inside the network that poisons the packets and alters original instructions of the PLC.

Overall Findings

After a thorough analysis of the situation, we have concluded as follows:

1. **Behavior of the Elevator and malfunctioning timeline:** The anomalous behaviors of the elevator have been recognized, named, and the time zero of the abnormal behavior has been located (section 3.1).

2. **Specific cause of malfunctioning:** The workstation bearing IP 192.168.10.164 has been compromised. A “backdoor” channel has been opened and malicious instructions have been sent to the PLC through that channel. We are unable to locate the name of the malware, but it is evident that, malware like “Emotet Trojan” creates a “Virtual Environment” to drop other applications into the infected system. The system was infected by “spam email”, which leads the victim to browse “suspicious website(s)” as defined in section 3.2.

3. **Any evidence of an inside attacker:** No evidence has been located to justify this objection.

4. **(A). Any attack evidence on the network:** ARP spoofing is evident as described in section 3.3 and 3.5.

   (B). Any attack evidence on the computer: Kristi Waynes's computer's IP address is 192.168.10.164, but we were able to find the host IP, 192.168.133.137, encoded in a RAM dump by utilizing "Bulk Extractor" and "Volatality v3 netscan.". This is the classic example of the trojan that able to hide itself by creating a virtual entity and establish communication channel with its server. Detail analysis has been conducted in section 3.2.

   (C). Any attack evidence on the PLC device: We discovered indications of tampering in the PLC system's external memory backups and observed code injection into the PLC system from a workstation. Detailed analysis has been conducted on section 3.4 and 3.5.

Biography

Md Ashiqur Rahman

Ph.D. student of Computer & Cyber Sciences at Augusta University, USA. He completed his M.Sc. in Computer Science & Engineering from North South University, Bangladesh. His research interests include natural language processing, grid computing, and data sciences.

mdrahman@augusta.edu

Dr. Gokila Dorai

Assistant Professor of Computer & Cyber Sciences at Augusta University, USA. She obtained her Ph.D. in Computer Science from Florida State University. Her research interests include digital forensics, security and privacy analysis, cybersecurity, and machine learning.

gdorai@augusta.edu