

Flag Table

Place the flags once you find them in the appropriate table entries below. Each category has a maximum of 20 points with each higher level of difficulty granting an increasing number of points. Maximum score for all challenges completed is 100 points.

| | Cryptography | Malware | Network Capture | Reverse Engineering | Steganography |
|---------------------------|-------------------------|----------------|------------------------|----------------------------------|--------------------------------|
| Level 1 (2 Points) | flag{backoff_malware} | passDs5Bu9Te7 | M0d1c0nF14G | lm | flag{covert_channel} |
| Level 2 (3 Points) | Wanna Cry ransomware | NA | admin, admin | ClippyHasReturned | Cookies_n_milk |
| Level 3 (4 Points) | flagslashdotdash | NA | HaveX RAT | Flag{infected} | 6 th file, R0075RU5 |
| Level 4 (5 Points) | did cicero say anything | NA | Port 1255 | c97ff22e75b6cf465b70ae0dddc8e773 | Angel Cries Quickly |
| Level 5 (6 Points) | | NA | p.sswordBasisk | flag{.} | Comment attribute: “nope” |

Explanation of Approaches

Include descriptions along with screen shots of the approaches you took to solve these challenges.

Cryptography

Level 1 – Orange Julius: Text: “**flag{backoff_malware}**” with key shift of 13. Used website: <https://www.xarg.org/tools/caesar-cipher/> to decipher the text. The character shift was: 13.

Level 2 – Block Chain

The decoded string from the given cipher is:

INTHISCOLUMNARCIPHERTHEFLAGIS**WANNACRY**WHICHISNOWAWELLKNOWNMALWARE

Wanna Cry Ransomware

Level 3 – DASH DOT COM

The flag is: **flagslashdotdash**

The morse code is:--. -.-.--. -.-. -.. --- -.. -.-.

The only variation found in the logs was that of the request type and the resource requested. Sometimes, the request specifies the image format other times it does not.

The apache log file was a morse code for the flag. The logs were converted into the morse code which was then a simple conversion process from morse code to human readable string text format.

Screenshots are attached below:

The screenshot shows a web browser window with the URL unit-conversion.info/text-tools/converters/convert-morse-code. The page title is "Convert Morse code to text". On the left, a sidebar lists various text conversion tools: ASCII to text converter, Hexadecimal to text, Convert text to binary, Convert Octal to Text, Convert Morse Code, A Letter to Uppercase, A Letter to Lowercase, Letter to Randomcase, Remove letter accents, Capitalize words, Capitalize sentence, Reverse text, Reverse words, Text to HTML, and Strip tags. The main area contains input fields for "Input data" (containing Morse code) and "Output: morse code to text" (containing "flagslashdotdash"). Below the input fields is a "Convert" button. At the bottom, a "About Convert Morse code to text tool" section provides a brief description of Morse code and its applications.

Level 4 – VIII A Small Example

“did cicero say anything”

Using RSA decyprion process, values: d=157, n=2773

Message, M= (4 bits) $^157 \bmod 2773$

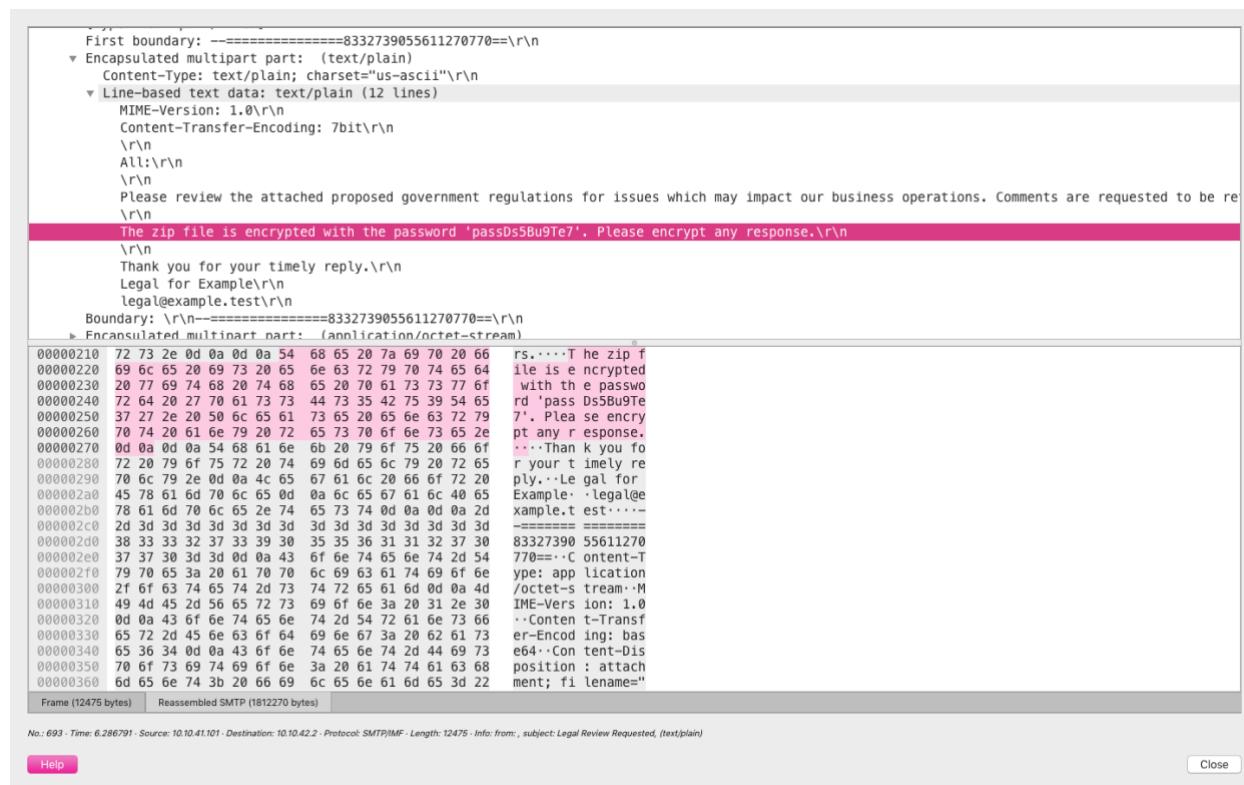
Level 5 – Big Blue Randu

Malware

Level 1: MLWR-1-PCAP

Using Wireshark packet forensics techniques

Extract file password: passDs5Bu9Te7



First boundary: =====8332739055611270770==\r\n

Encapsulated multipart part: (text/plain)

Content-Type: text/plain; charset="us-ascii"\r\n

Line-based text data: text/plain (12 lines)

MIME-Version: 1.0\r\n

Content-Transfer-Encoding: 7bit\r\n

\r\n

All:\r\n

\r\n

Please review the attached proposed government regulations for issues which may impact our business operations. Comments are requested to be re

\r\n

The zip file is encrypted with the password 'passDs5Bu9Te7'. Please encrypt any response.\r\n

\r\n

Thank you for your timely reply.\r\n

Legal for Example\r\n

legal@example.test\r\n

Boundary: \r\n

Encapsulated multipart part: (application/octet-stream)

00000210 72 73 2e 0d 0a 0d 0a 54 68 65 20 7a 69 70 20 66 rs.....T he zip f

00000220 69 6c 65 20 69 73 20 65 6e 63 72 79 70 74 65 64 ile is e ncrypted

00000230 20 77 69 74 68 20 74 68 65 20 70 61 73 73 77 6f with th e passwo

00000240 72 64 20 27 70 61 73 73 44 73 35 42 75 33 54 65 rd 'pass Ds5Bu9Te

00000250 37 27 2e 20 50 6c 65 61 73 65 20 65 6e 63 72 79 7'. Plea se encry

00000260 70 74 20 61 6e 79 20 72 65 73 70 6f 6e 73 65 2e pt any r esponse.

00000270 0d 0a 0d 0a 54 68 61 6e 6b 20 79 6f 75 20 66 6f ...Than k you fo

00000280 72 20 79 6f 75 72 20 74 69 6d 65 6c 79 20 72 65 r your t imely re

00000290 70 6c 79 2e 0d 0a 4c 65 67 61 6c 20 66 6f 72 20 ply, ..Le gal for

000002a0 45 78 61 6d 70 6c 65 0d 0a 6c 65 67 61 6c 40 65 Example. .legal@e

000002b0 78 61 6d 70 6c 65 2e 74 65 73 74 0d 0a 0d 0a 2d xample.t est...-

000002c0 2d 3d =====

000002d0 38 33 33 32 37 33 39 30 35 35 36 31 31 33 37 30 83327390 55611270

000002e0 37 37 30 3d 3d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 770=-.C ontent-T

000002f0 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e ype: app lication

00000300 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a 4d /octet-s tream-M

00000310 49 4d 45 2d 56 65 72 73 69 6f 6e 3a 20 31 2e 30 IME-Vers ion: 1.0

00000320 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 .Content-T-Transf

00000330 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 62 61 73 er-Encod ing: bas

00000340 65 36 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 e64. Content-Dis

00000350 70 6f 73 69 74 69 6f 6e 3a 20 61 74 74 61 63 68 position : attach

00000360 66 65 66 74 3b 20 66 69 6c 65 66 61 6d 65 3d 22 ment; fi lename="

Frame (12475 bytes) Reassembled SMTP (1812270 bytes)

No.: 623 - Time: 6.286791 - Source: 10.10.41.101 - Destination: 10.10.42.2 - Protocol: SMTP|IMF - Length: 12475 - Info: from: , subject: Legal Review Requested, (text/plain)

Help Close

Level 2:

Not provided

Level 3:

Not provided

Level 4:

Not provided

Level 5:

Not provided

Network Capture

Level 1 – Modicon-FTP

Password is: M0d1c0nF14G

```
► Frame 163: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
► Ethernet II, Src: Apple_16:5b:bd (c8:e0:eb:16:5b:bd), Dst: CheckPoi_39:de:5b (00:1c:7f:39:de:5b)
► Internet Protocol Version 4, Src: 10.200.1.174, Dst: 10.50.1.52
► Transmission Control Protocol, Src Port: 60115, Dst Port: 21, Seq: 20, Ack: 47, Len: 18
▼ File Transfer Protocol (FTP)
  ▼ PASS M0d1c0nF14G\r\n
    Request command: PASS
    Request arg: M0d1c0nF14G
[Current working directory: ]
```

```
0000  00 1c 7f 39 de 5b c8 e0 eb 16 5b bd 08 00 45 00  ...9 [ ... [ ... E ...
0010  00 3a f5 e7 40 00 40 06 2c fb 0a c8 01 ae 0a 32  : ... @ @ , .....2
0020  01 34 ea d3 00 15 40 7d b4 d5 c2 8a a1 ec 50 18  4 ... @ ) .....P ...
0030  00 e5 74 ad 00 00 50 41 53 53 20 4d 30 64 31 63  ..t...PA SS M0d1c
0040  30 6e 46 31 34 47 0d 0a  0nF14G ..
```

Help

Close

Level 2 – Modicon-HTTP

Password is: admin, username:admin

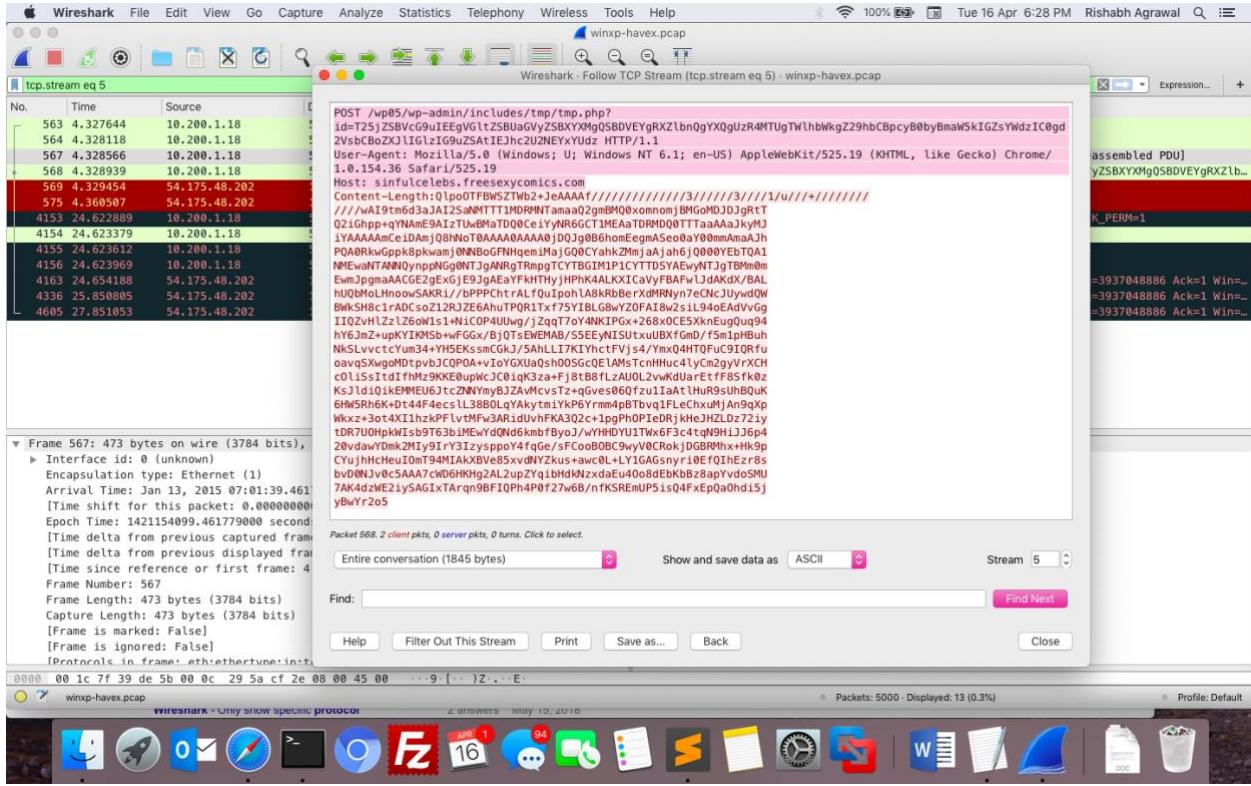
```

[TCP Segment Len: 488]
Sequence number: 1256 (relative sequence number)
[Next sequence number: 1744 (relative sequence number)]
Acknowledgment number: 4680 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
▶ Flags: 0x018 (PSH, ACK)
Window size value: 16384
[Calculated window size: 262144]
[Window size scaling factor: 16]
Checksum: 0x6394 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▼ [SEQ/ACK analysis]
  [iRTT: 0.123463000 seconds]
  [Bytes in flight: 488]
  [Bytes sent since last PSH flag: 488]
▼ [Timestamps]
  [Time since first frame in this TCP stream: 10.785136000 seconds]
  [Time since previous frame in this TCP stream: 3.912228000 seconds]
  TCP payload (488 bytes)
▼ [HyperText Transfer Protocol]
  ▼ GET /secure/embedded/builtin?submit=Configure+SNMP HTTP/1.1\r\n
    ▼ [Expert: Info (Chat/Sequence): GET /secure/embedded/builtin?submit=Configure+SNMP HTTP/1.1\r\n]
      [GET /secure/embedded/builtin?submit=Configure+SNMP HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
    ▼ Request URI: /secure/embedded/builtin?submit=Configure+SNMP
      Request URI Path: /secure/embedded/builtin
    ▼ Request URI Query: submit=Configure+SNMP
      Request URI Query Parameter: submit=Configure+SNMP
      Request Version: HTTP/1.1
    Host: 10.50.1.52\r\n
    Connection: keep-alive\r\n
  ▼ Authorization: Basic YWRtaW46YWRtaW4=\r\n
    Credentials: admin:admin
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
    Referer: http://10.50.1.52/html/english/setup/menu.htm\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
  \r\n
  [Full request URI: http://10.50.1.52/secure/embedded/builtin?submit=Configure+SNMP]
  [HTTP request 4/12]
  [Prev request in frame: 324]
  [Response in frame: 347]
  0000  00 1c 7f 39 05 b4 10 9f da f8 4b 08 00 45 00  ... 9: [ ... ] K-E
  0010  01 20 37 3a 40 00 40 06 ea 2a 0a c8 01 56 0a 32  .7:@ @ *-*P
  0020  01 34 da 3e 00 50 e5 0e 04 77 c1 d9 f2 05 50 18  .4> P. ....P
  0030  40 00 63 94 00 00 07 45 54 20 21 73 65 63 75 72  @c GE T /secu
  0040  65 2f 62 6d 62 65 64 64 65 64 2f 62 75 69 66 74  r/embbedd ed/buil
  0050  69 63 61 74 66 62 60 69 74 63 63 60 66 69 67  in?subm t=Configure
  0060  75 72 65 2b 53 6d 4d 50 20 48 54 54 50 31 26  un?SNMP HTTP/1.1
  0070  75 72 65 2b 53 6d 4d 50 20 31 30 2e 31 26 1- Host: 10.50.1
  0080  2e 25 32 0d 0a 43 6f 6e 66 65 63 74 69 61 6e 3a  .52- Con nection:
  0090  20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 75 74  keep-al iive-Aut
  00a0  68 6f 72 69 73 61 74 69 6f 6e 3a 20 42 61 73 69  horizati on; Bas
  00b0  63 20 59 57 62 74 61 57 34 36 59 57 52 74 61 57  c YWRtaW 46YWRtaW
  00c0  34 3d 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74  4=...Acc ept: text
  00d0  21 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 67  /html,ap plicatio
  00e0  6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c  n/xhtml+xml,appl
  00f0  69 63 61 74 69 66 67 2f 6d 66 3b 71 3d 30 2e  ication/ xml;q=0.
  0100  39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a  9,image/ webp,*/*
  0110  3b 71 3d 30 2e 38 0d 0a 55 73 65 72 2d 41 67 65  :q=0.8.. User-Age
  0120  6e 74 3a 20 4d 6f 7a 69 6c 61 2f 35 2e 30 20  nt: Mozil la/5.0
  0130  28 4d 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 65  (Macintosh; Inte
  0140  6c 20 4d 61 63 20 4f 53 20 58 20 31 30 5f 38 5f  l Mac OS X 10_8_
  0150  35 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35  5) Apple WebKit/5
  0160  33 37 26 33 30 28 28 4b 48 54 4d 4c 2c 20 6c 69  37.30 (KHTML, li
  0170  6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65  ke Gecko ) Chrome
  0180  2f 33 39 2e 3b 32 31 37 31 26 39 35 20 53 61  /39.0.21 71.95 Sa
  0190  66 61 72 69 2f 35 33 37 26 33 36 0d 0a 52 65 66  fari/537 .36·Ref
  01a0  65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 31 30 2e  erer: ht tp://10.
  01b0  35 20 31 2e 25 32 2f 68 74 6d 6c 2f 65 6e 67  50.1.52/ html/eng
  01c0  6c 20 31 2e 25 32 2f 68 74 6d 6c 2f 65 6e 67  lish/set up/menu
  01d0  64 69 6d 68 2f 73 65 74 75 50 21 6d 65 66 75 2e  /html-Adapt-Enc
  01e0  64 69 6d 68 2f 73 65 74 65 70 2c 20 64 65 66 6c  ding/62,ip,defl
  01f0  61 74 65 2c 20 73 64 63 68 0d 0a 41 63 63 65 70  ate, sdc h-Accp
  0200  74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 66 2d 55  t-Langua ge: en-U
  0210  53 2c 65 6e 3b 71 3d 30 2e 38 0d 0a 0d 0a 5, en;q=0 .8... .

```

Level 3 – WinXP-HAVEX

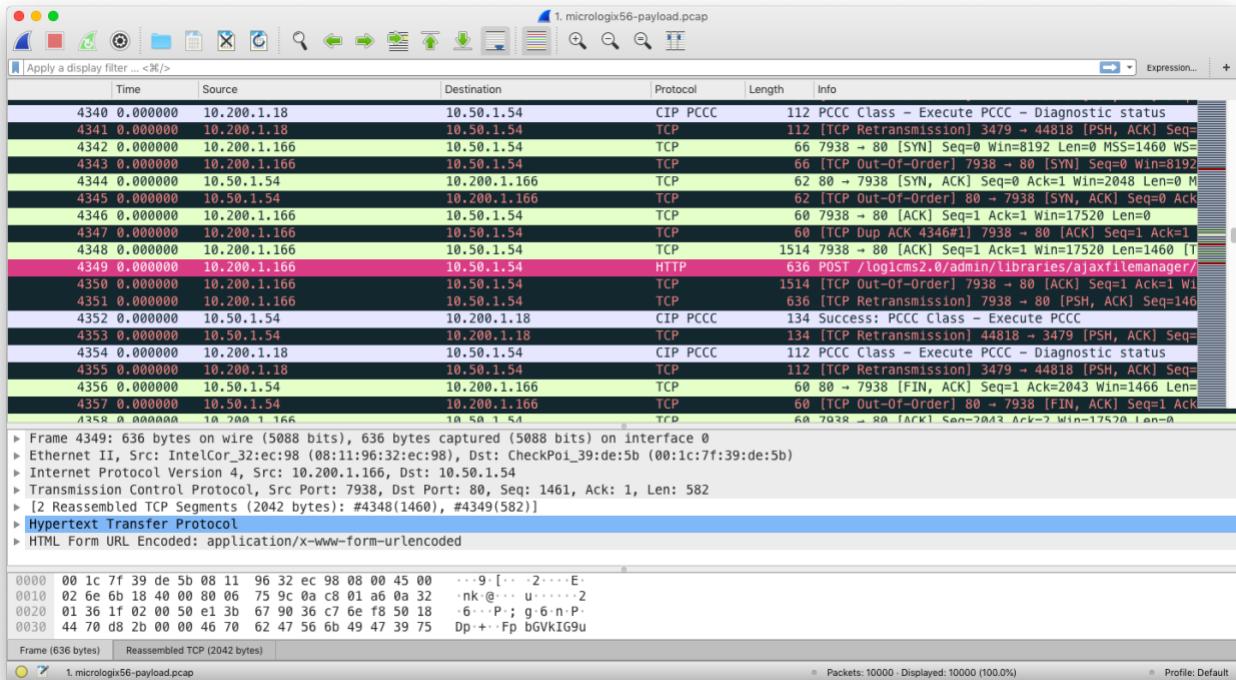
Havex is a Remote Access Trojan (RAT) that in this case is attempting to install a backdoor access by putting the php file in the server.



Level 4 – MICROLOGIX56

Port: 1255

Packet number 4349 is trying to post a payload at the destination. The backdoor is most likely the port 1255. Here, **10.50.1.54** is the target machine. Screenshot below:



Level 5 – BACNET-COVERT

I started out with just looking at the pcap with tcpdump:

```
tcpdump -nn -l -r 2.\ bacnet-covert.pcap | less
```

I then looked at the ascii content of the pcap with the command:

```
tcpdump -nn -l -A -r 2.\ bacnet-covert.pcap | less
```

Some ascii printable in the traffic to port 47808 and the word SpotUdp in the traffic to port 5762. But port number 47808 is the default port for BACnet.

On Wireshark, we can see all traffic to 47808 decoded as “Unconfirmed-REQ who-Is xx xx” request.

Next, we move to separating the last number from the traffic and convert it to both binary and hex.

```
00000000 86 d6 fb 87 b6 b7 91 70 d5 c7 db e3 95 fc ce 00 |.....p.....|
00000010 b0 cb e4 82 e1 92 e5 73 f6 d5 bd 84 d3 9b bb 73 |.....s.....s|
00000020 90 df c0 d9 f4 ee a1 77 ab d5 85 e9 82 d8 b9 6f |.....w.....o|
00000030 e4 ff 87 ba 8a a4 f2 72 e6 aa b7 e1 a7 c7 c9 64 |.....r.....d|
00000040 a3 82 e2 ff f4 d5 a8 42 a5 b0 e7 92 d1 df 85 61 |.....B.....a|
00000050 95 fc 96 9b 9b ca d5 73 84 c4 a6 9d 9a b8 c2 69 |.....s.....i|
00000060 e0 a2 fe e3 94 96 88 73 99 e6 c6 8e d1 ff e3 6b |.....s.....k|
```

Message therefore is: “p.sswordBasisk”

Reverse Engineering

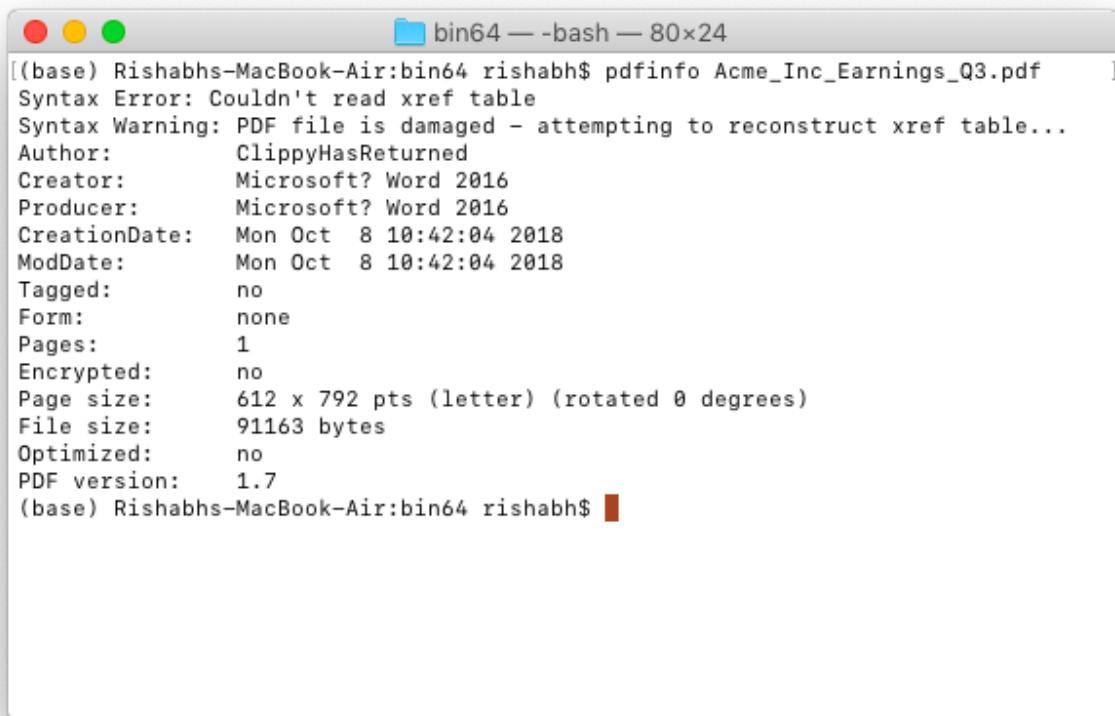
Level 1 – Script Kiddie:

Password is: “Im”, the password is a substring of characters from the password variable.

Level 2 – The PDF Your Parents Warned You About I

Author: ClippyHasReturned

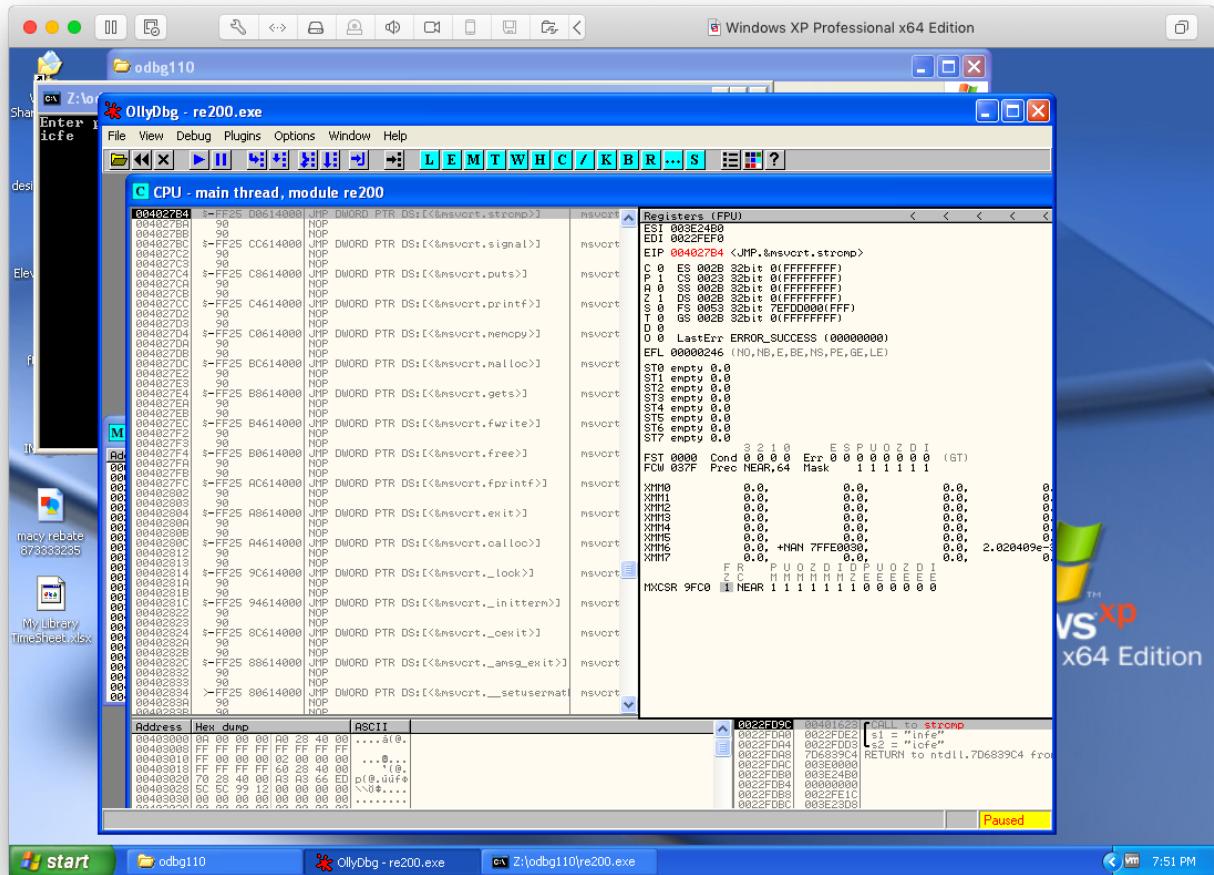
Using XpdfReader, it was an easy task to find the Author of the file. Screenshot attached.

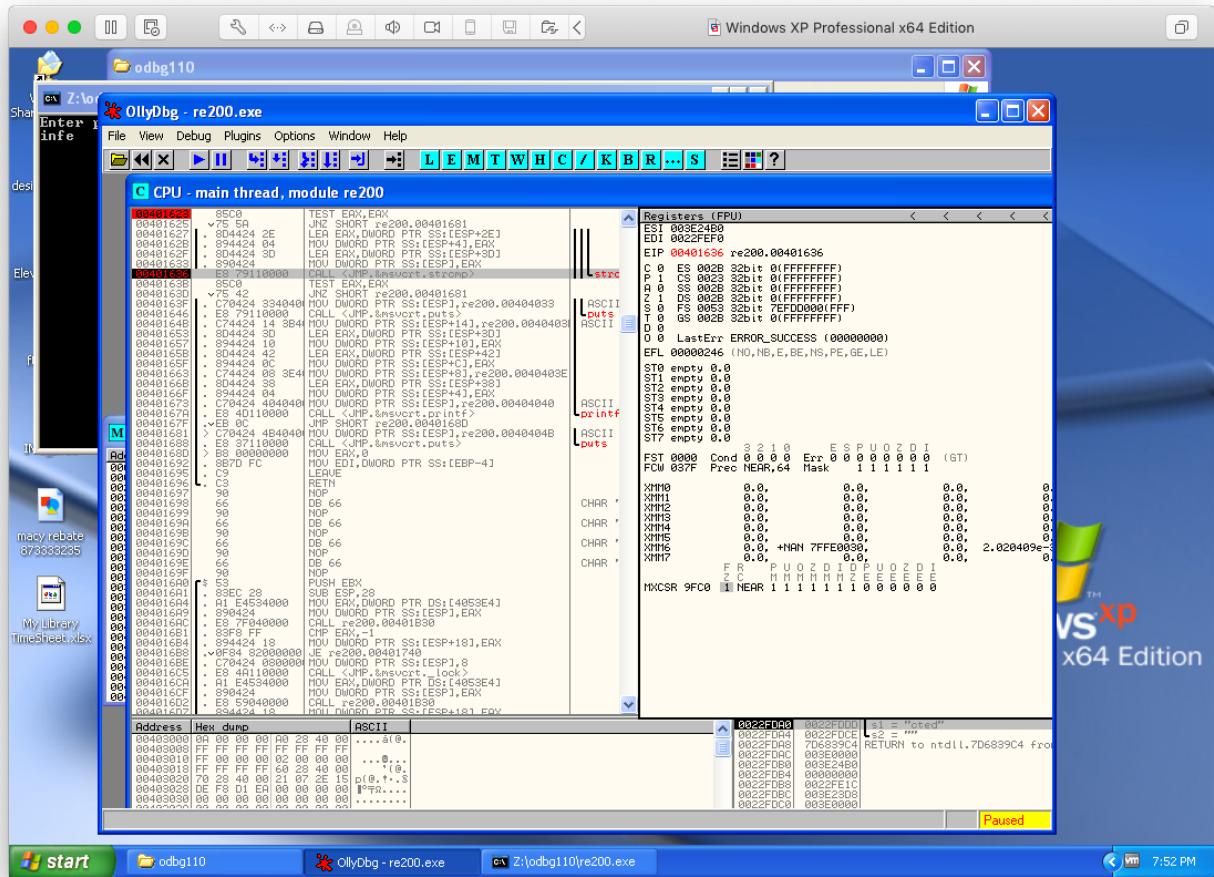


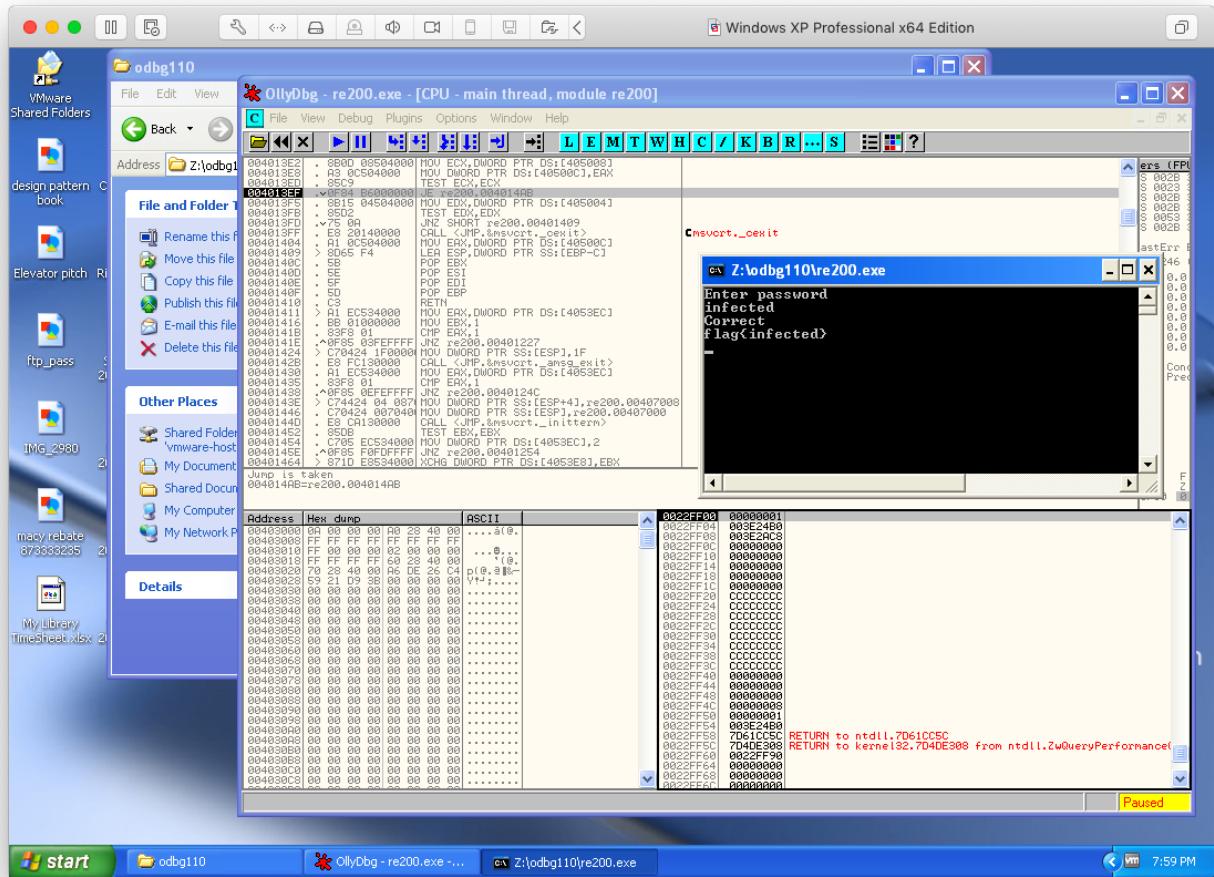
```
bin64 — -bash — 80x24
[(base) Rishabhs-MacBook-Air:bin64 rishabh$ pdfinfo Acme_Inc_Earnings_Q3.pdf]
Syntax Error: Couldn't read xref table
Syntax Warning: PDF file is damaged - attempting to reconstruct xref table...
Author: ClippyHasReturned
Creator: Microsoft? Word 2016
Producer: Microsoft? Word 2016
CreationDate: Mon Oct 8 10:42:04 2018
ModDate: Mon Oct 8 10:42:04 2018
Tagged: no
Form: none
Pages: 1
Encrypted: no
Page size: 612 x 792 pts (letter) (rotated 0 degrees)
File size: 91163 bytes
Optimized: no
PDF version: 1.7
(base) Rishabhs-MacBook-Air:bin64 rishabh$
```

Level 3 – Split Ends

The task involved reverse engineering the executable build file. Tools used for this operation: Ollydbg, run on Windows XP as guest OS on top of MAC host OS. Breakpoints were created at the strcmp() and the Z-flag was turned to 1 which then caused the register to reveal the value of the source it is comparing to. Password was revealed in a span of 2 iterations where each iteration revealed 4 characters of the password. After a breakpoint was reached, each step was manually iterated to see the output in real-time on the DOS window. Screenshots are attached below:







Level 4 – The PDF Your Parents Warned You About II

The pdf file had an base64 encoded powershell script. The script basically computes the MD5 hash for the string: “*Please insert key*”

Hash: **c97ff22e75b6cf465b70ae0dddc8e773**

Script and the screenshot are attached below:

rumkin.com 43

Stuff The (16) Gaurav... Base64 WriteCodeO... Another For... PowerShell... PowerShell... MD5 Hash... +

Base64

Rumkin.com >> Web-Based Tools >> Ciphers and Codes

Search: INDEX

Base64, also known as MIME encoding, translates binary into safe text. It is used to send attachments in email and to change small bits of unsafe high-character data into stuff that is a lot nicer for text-based system.

Decrypt ↻

vACAAIgBGAGwAYQBnACAAbQBhAHkAIABIAGUAIAkAGgAYQBzAGgAlgA7ACAAUgBiAGEAZAAAtAGgAbwBzAHQAIAAAtAFAAcgBvAG0AcA
B0ACAAIgBSAGUAbQBvAHYAZQAgAGQAYQBzAGgAZQBzACAAcAbYAGkAbwByACAAAdAbvACAAcwb1AGIAbQBpAHMAcwBpAG8AbgAuA
CAARQBuAHQAZQByACAAAdAbvACAAZQB4AGkAdAAIA

This is your encoded or decoded text:

```
$var1 = Read-Host "Please insert key"; $md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider; $utf8 = new-object -TypeName System.Text.UTF8Encoding; $hash = [System.BitConverter]::ToString($md5.ComputeHash($utf8.GetBytes($var1))); echo "Flag may be $hash"; Read-host -Prompt "Remove dashes prior to submission. Enter to exit"
```

Washington Post's Style Invitational 2003 Winner:
Reintarnation: Coming back to life as a hillbilly.

Tyler Akins <fidian@rumkin.com>
[Legal Info](#)

INDEX

- Affine
- Atbash
- Baconian
- Base64
- Bifid
- Caesar
- Keyed
- ROT13
- Column Trans.
- Double
- Übchi
- Cryptogram
- Gronsfeld
- Morse
- Numbers
- One Time Pad
- Playfair
- Railfence
- Rotate
- Skip
- Substitution
- Vigenere
- Keyed
- Autokey
- Crypto Solver
- Frequency
- Manipulator

```

65 6E 41 63 /4 69|b| 6E Z0 3C|3C ZF 53 20|Z| 4C b1 /5|b| b3 68 2F|5| 69 6E 20
69 6E 64 6F 77 73|50 6F 77 65|72 53 68 65|6C 6C 5C 5C|76 31 2E 30|5C 5C 70 6F
6E 63 6F 64 65 64|63 6F 6D 6D|61 6E 64 20|55 41 42 76|41 48 63 41|5A 51 42 79
42 31 41 48 51 41|61 51 42 76|41 47 34 41|55 41 42 76|41 47 77 41|61 51 42 6A
42 76 41 48 41 41|63 67 42 76|41 47 59 41|61 51 42 73|41 47 55 41|49 41 41 74
41 67 41 47 67 41|61 51 42 68|41 47 51 41|5A 51 42 75|41 43 41 41|41 51 42 46
42 41 47 51 41|49 41 42 48|41 45 45 41|51 67 41 79|41 45 45 41|52 77 42 46
42 75 41 47 63 41|51 51 42 47|41 45 68 41|51 51 42 61|41 46 45 41|51 67 42 6F
42 42 41 47 4D 41|64 77 42 43|41 44 41 41|51 51 42 44|41 45 45 41|51 51 42 4A
42 42 41 45 67 41|54 51 42 42|41 46 6F 41|55 41 42 42|41 47 63 41|51 51 42 48
42 6E 41 45 49 41|40 41 42 42|41 45 40 41|51 51 42 42|41 47 45 41|64 77 42 43
42 42 41 45 45 41|53 67 42 42|41 45 49 41|64 41 42 42|41 45 63 41|55 51 42 42
42 31 41 45 45 41|52 77 42 56|41 45 45 41|5A 51 42 33|41 45 45 41|64 41 42 42
42 5A 41 48 63 41|51 67 41 77|41 45 45 41|51 77 42 42|41 45 45 41|54 41 42 52
42 46 41 44 51 41|51 51 42 54|41 46 45 41|51 67 42 30|41 45 45 41|52 77 42 56
42 43 41 44 41 41|51 51 42 48|41 46 55 41|51 51 42 69|41 46 45 41|51 51 42 31
42 42 41 47 4D 41|5A 77 42 43|41 48 41 41|51 51 42 49|41 46 45 41|51 51 42 6C
42 42 41 45 67 41|51 51 42 42|41 47 51 41|51 51 42 43|41 46 59 41|51 51 42 48
42 42 41 45 49 41|4E 51 42 42|41 45 40 41|4E 41 42 42|41 46 51 41|55 51 42 43
42 72 41 45 45 41|59 77 42 42|41 45 49 41|4D 41 42 42|41 45 63 41|4F 41 42 42
42 77 41 45 45 41|52 77 42 4E|41 45 45 41|57 67 42 52|41 45 49 41|55 51 42 42
42 61 41 45 45 41|51 67 42 73|41 45 45 41|53 41 42 4A|41 45 45 41|54 77 42 33
42 48 41 46 68 41|51 51 42 50|41 45 45 41|51 51 42 6E|41 45 45 41|52 41 41 77
42 42 41 48 51 41|51 51 42 48|41 44 67 41|51 51 42 5A|41 47 63 41|51 67 42 78
42 42 41 45 77 41|55 51 42 43|41 46 55 41|51 51 42 49|41 47 73 41|51 51 42 6A
42 42 41 45 63 41|56 51 42 42|41 45 68 41|51 51 42 43|41 46 51 41|51 51 42 49
42 52 41 45 45 41|64 51 42 42|41 45 59 41|55 51 42 44|41 46 6F 41|55 51 42 43
42 52 41 45 45 41|55 67 42 6E|41 45 45 41|4E 41 42 42|41 45 55 41|56 51 42 42
42 77 41 45 45 41|52 77 41 30|41 45 45 41|57 67 42 33|41 45 45 41|4E 77 42 42
42 6A 41 48 63 41|51 67 42 76|41 45 45 41|51 77 42 42|41 45 45 41|55 41 42 52
42 49 41 45 30 41|51 51 42 68|41 45 45 41|51 67 42 73|41 45 45 41|52 77 41 77
42 43 41 45 51 41|51 51 42 48|41 44 67 41|51 51 42 69|41 47 63 41|51 67 41 79
42 42 41 47 4D 41|5A 77 42 43|41 47 51 41|51 51 42 45|41 47 38 41|51 51 42 50
42 42 41 45 67 41|53 51 42 42|41 47 45 41|55 51 42 43|41 48 55 41|51 51 42 48
42 42 41 45 45 41|4D 51 42 42|41 45 40 41|4E 41 42 42|41 46 45 41|64 77 42 43
42 52 41 45 45 41|57 67 42 52|41 45 49 41|53 51 42 42|41 45 63 41|52 51 42 42
41 78 41 45 45 41|53 41 42 52|41 45 45 41|57 67 42 6E|41 45 45 41|4E 41 42 42
42 52 41 47 63 41|51 67 41 31|41 45 45 41|53 41 42 52|41 45 45 41|57 67 42 52
42 48 41 45 55 41|51 51 42 6A|41 47 63 41|51 51 42 34|41 45 45 41|51 77 42 72
42 43 41 47 77 41|51 51 42 48|41 45 30 41|51 51 42 68|41 45 45 41|51 67 42 32
42 42 41 46 6B 41|55 51 42 43|41 47 34 41|51 51 42 44|41 45 45 41|51 51 42 69
42 42 41 45 63 41|56 51 42 42|41 45 6B 41|51 51 42 42|41 47 73 41|51 51 42 48
88116...%EUF..100 0 obj.<</OpenAction <</S /Launch /Win
<</F (C:\Windows\WindowsPowerShell\v1.0\powershell.exe /P (powershell -encodedcommand UABVbAHCbAzbQBy
AFMaaABLAGwAbAAGAC0ARQB4AGUAYwB1AHQAaQBvAG4AUAbvAGwAaQBj
AHKAIAb1AHKAcbAbhMacwAgAC0AbgBvAHAAcgbvAGYAAqBsAGUATAA
AHcAaQbAQBwB3AHMAdAB5AGwA0QAgAGaQbKAGQaQbZQBuACAALQB
AG4AYwBvAGQAZQbKAEMAbwBTAGAYQbQAG0IABKAEAAQgAyAEEARwB
AEEAYwBnAEEAeABBAEAMQ0QBBFAFAUQBBAGcAQBGAEKAQQbAaFEEQgB
AEEARwBRAEAEATABRAEIASQBBAEcAOABBAGMAdwBCADAAQQBDAEEAQQB
AGcA0gBRAEAEARwB3AEEARwBRAEIAaABBAEgATQBBAf0AUQBBAGcAQB
AGsAQB1AGcA0gB6AEARwBRAEIAaEAMABBAEAMQ0BBAEAdwBC
AGwAQB1AGsAQBjAGcAQ0A3EEAqBBAEASgBBAEIAdABBAGcAUQBB
AE4AUQBBAGcAQ0BEBADAAQQBjAEEAqgB1AEEARwBVAEEA2AB3AEAAdABB
AEcAOABBFAKZwBCAHEAQ0QbHAFUaQ0QbZAHcAqgAwAEEAqgBBAEAEATABR
AEIAVQBBAEgAawBBAGMAQ0BCAGwAQBFAf0AQ0QbZAFEAqgB0AEEARwB
AEEASQBBAEIAVABBAGeAawBBAGMAdwBCADAAQQBbHAFUaQ0QbIAFEEQ0Qb1
AEEARgBNAEEAwBRAEIAgB8AEGAVQBAGMAZwBCAHAQ0QbIAFEEQ0Qb1
AEEFAQb1AEAEARwBNAEAEABBAEgAQBbAEGQbCAGhYQQBH
AGMAQb1AGcA0gB0AEEASBAAEAYwBBAEIAQ0BBAEAMANABBAEAc0QbC
AEUAQb1AEFAUQ0BRAHcAqgB5AEEASBArAEEAYwBBAEIAQ0BBAEAc0QbC
AFUAdwBCAGwAQBIAkQbKAAGcA0gBwAEEARwBNAEEAWgBRAEIAUQbB
AEgASQBBAGIAdwBCADIAQ0QbHAGsAQ0BAAEAEQgB0AEEASABjAEEATwB3
AEAAzWBBAAEAMQ0BBAEgAQBbAEEAQBbHAFkAQBPAEAAQ0QbNAEEAARAAw
AEEASQBBAEIAQ0BBAEgAQBbAEGQbCAGhYQQBH
AEEFAQb1AEQbBAGQd0BBAEQAQ0QbHADgAQBbAEEAQBbAEEA0AEEAWgB3AEAAwB
AEEAZwBCAGoAQBbHADgAQBbAEEAQBbAEEA0AEEAWgB3AEAAwB
AEMQAQBBAAEQAQ0BbHAG8AQ0QbHAFUaQ0QbJAHCgAqgBvAEEAqgBBAEAEUABR
AEEAAzWBBAEYAcwBBAFUdwBCADUAQ0BIAE0Q0BKAEEAqgB0AEEARwA
AEEATABnAEEIAQ0BbHAGcA0wBBAEQAQ0QbHADgAQBbA0iAGcA0gAy
AEEARwBVAEEAYwBnAEEIAQ0BBAEAcAVQBAGMAZwBCAGQ0QbEAG8AQ0QbP
AGcA0gBVAEEARwA4AEAEQb3AEIAQ0BBAEgASQBBAGEA0Q0QbCAGHUAQ0Qb
AGMAQb1AEEQ0QbRrAEEArwAEEA0QbBAAEAMQ0BBAEAMANABBAEAc0QbC
AHYAAQbHADAAQ0BjAEEAqgAxAEEASABRAEAEwBRAEIAQ0BBAEAc0QbC
AGMAdwBCAG8AQ0BbHADgAQBbAEEAQBbAEEA0AEEAWgBnAEEENAB
AEMANABBAFIAdwBCAGwAQB0QbIAFEAQB0RAGcAqgA1AEEAQbAEEA0QbC
AEIAgBBAEAMZwBBAEoAQB0CADIQAQ0BbHAFUaQ0QbJAGcA0QbB4AEAEQwB
AEEASwBRAEAcABBAEQAQcwbBAEKAQ0QbCAGwAQBbHAE0AQBbHAAEAEQgB
AEEA0QwBBAEAEASQbNAEIARwBBAEAcdwBBAfKAQ0BbCAG4AQ0BbDAEEAQ0b1
AEFA0gB0AEEASABrAEEASQBBAEIAaQBBAEcAVQBBAEKAQ0QbBAGsAQ0QbH

```

Manually computed the MD5 hash for the string. The console for the script gave me some error but it was easy to understand what the program is doing. Screenshot for that is also attached below:

The screenshot shows a TIO run interface with a PowerShell session. The script reads a key, hashes it, and prints the hash. The output window shows the key being inserted and the resulting hash. The debug window shows a null argument exception for the GetBytes method. The timing and exit code are also displayed.

```

$var1 = Read-Host "Please insert key";
$md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider;
$utf8 = new-object -TypeName System.Text.UTF8Encoding;
$hash = [System.BitConverter]::ToString($md5.ComputeHash($utf8.GetBytes($var1)))

echo "Flag may be $hash";
# Read-host -Prompt "Remove dashes prior to submission. Enter to exit"

```

▶ Footer

▶ Input

▶ Arguments

▼ Output

Please insert key:
Flag may be

▼ Debug

```

Exception calling "GetBytes" with "1" argument(s): "Array cannot be null.
Parameter name: chars"
At /tmp/home/.code.tio.ps1:4 char:1
+ $hash = [System.BitConverter]::ToString($md5.ComputeHash($utf8.GetByt ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ArgumentNullException

```

```

Real time: 1.479 s
User time: 0.927 s
Sys. time: 0.220 s
CPU share: 77.55 %
Exit code: 0

```

Level 5 – Rock Scissors Paper Lizard Spock

Using OxED for MacOS, the .exe file was opened and analyzed. The flag found is: “flag{.}”. Screenshot below:

The screenshot shows the assembly dump of a .exe file in OxED. The flag{.} string is highlighted in pink in the assembly dump, indicating its location in memory.

Steganography

Level 1 – Moo Cow

flag{covert_channel}
Screenshot attached below:

white.bmp

Hex Text search

Save Copy Cut Paste Undo Redo

Go To Offset Find (Text search)

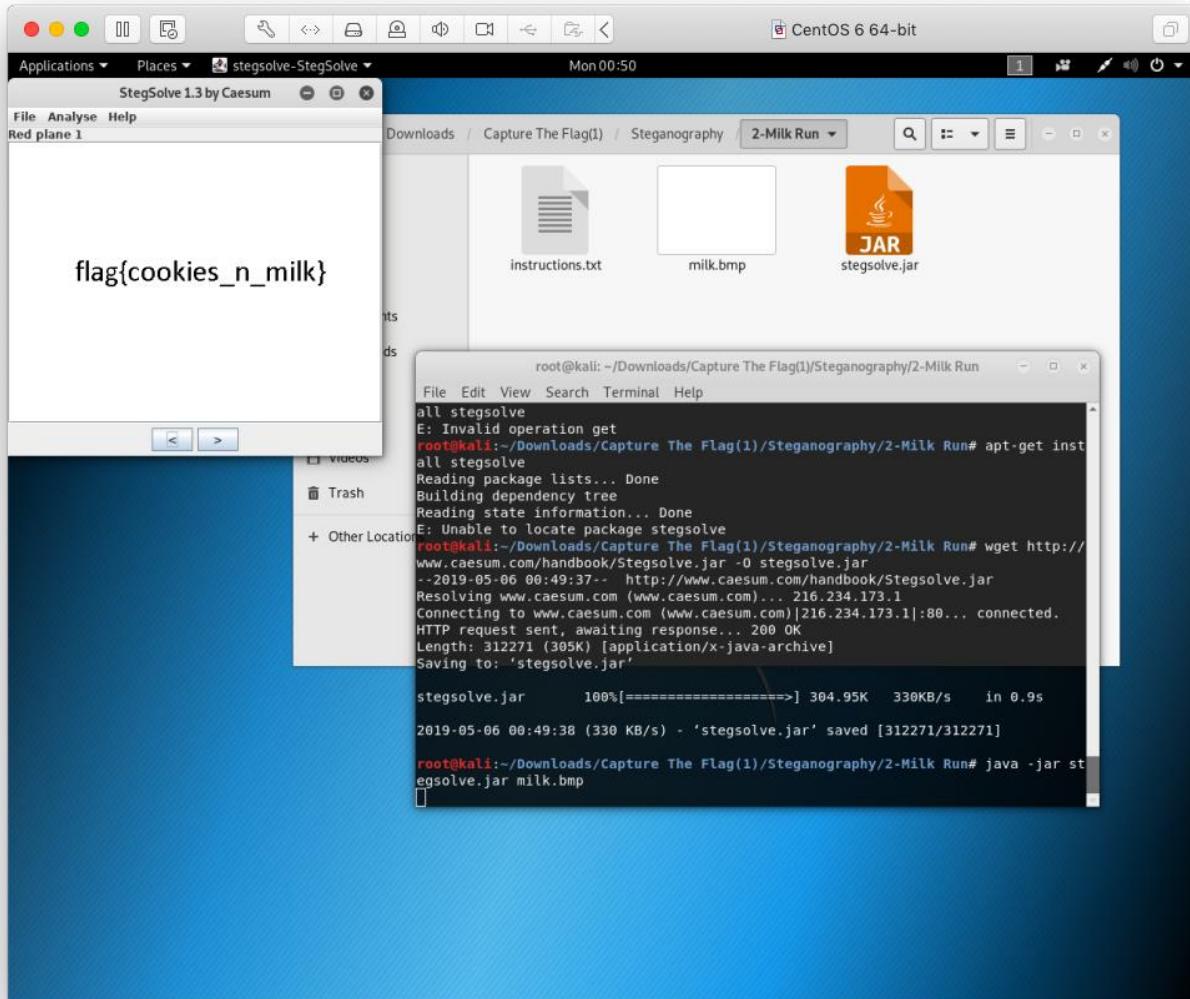
| Type | Value |
|-----------------|------------|
| 8 bit signed | 102 |
| 8 bit unsigned | 0x66 |
| 16 bit signed | 27750 |
| 16 bit unsigned | 0x6C66 |
| 32 bit unsigned | 0x67676C66 |

Hex Little Endian Insert ASCII Offset: 26 Selection: 14

Level 2 – Milk Run

Flag{cookies_n_milk}

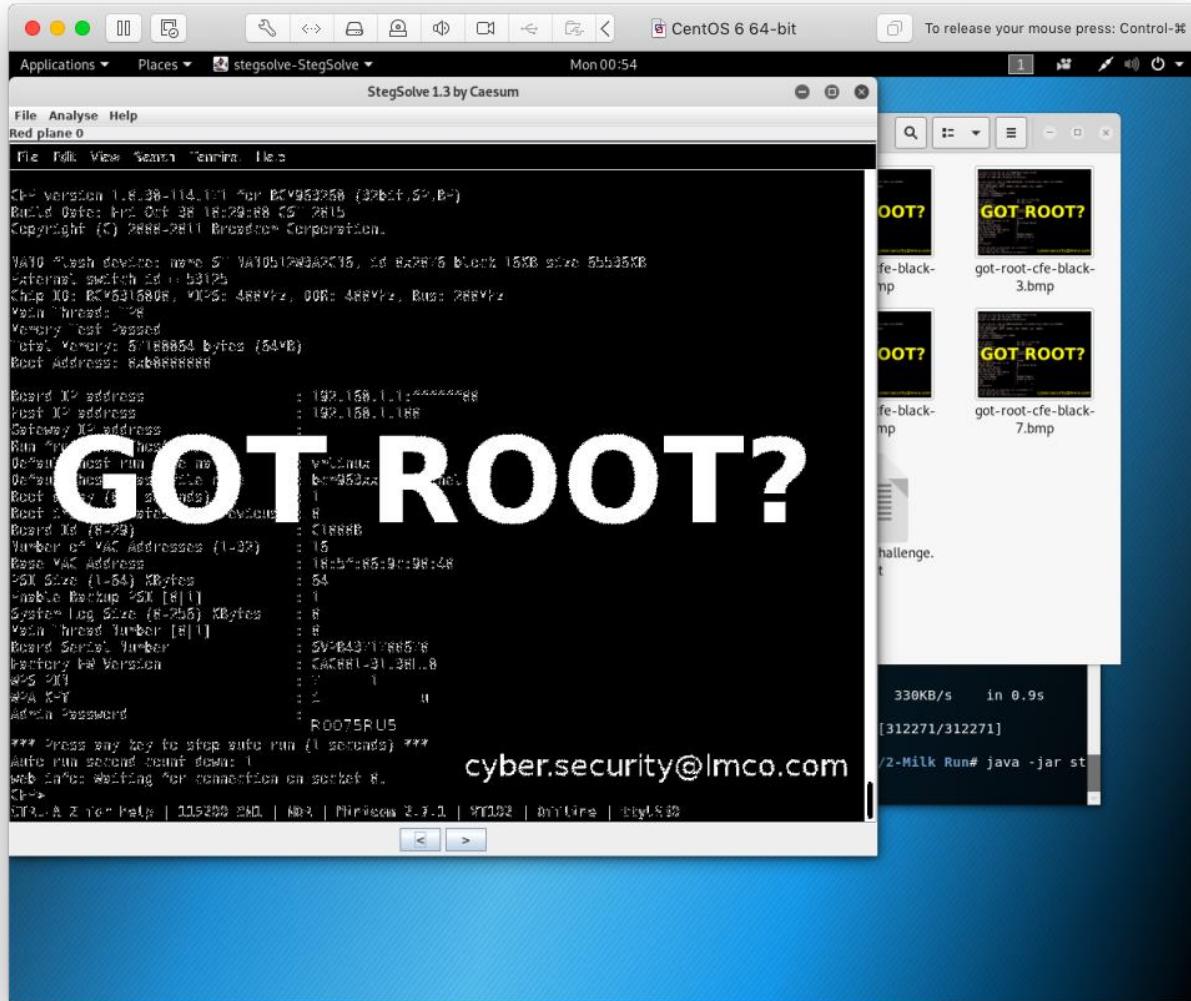
Using StegSolve in Kali Linux, we were able to change color channel and expose the hidden flag for the particular image.

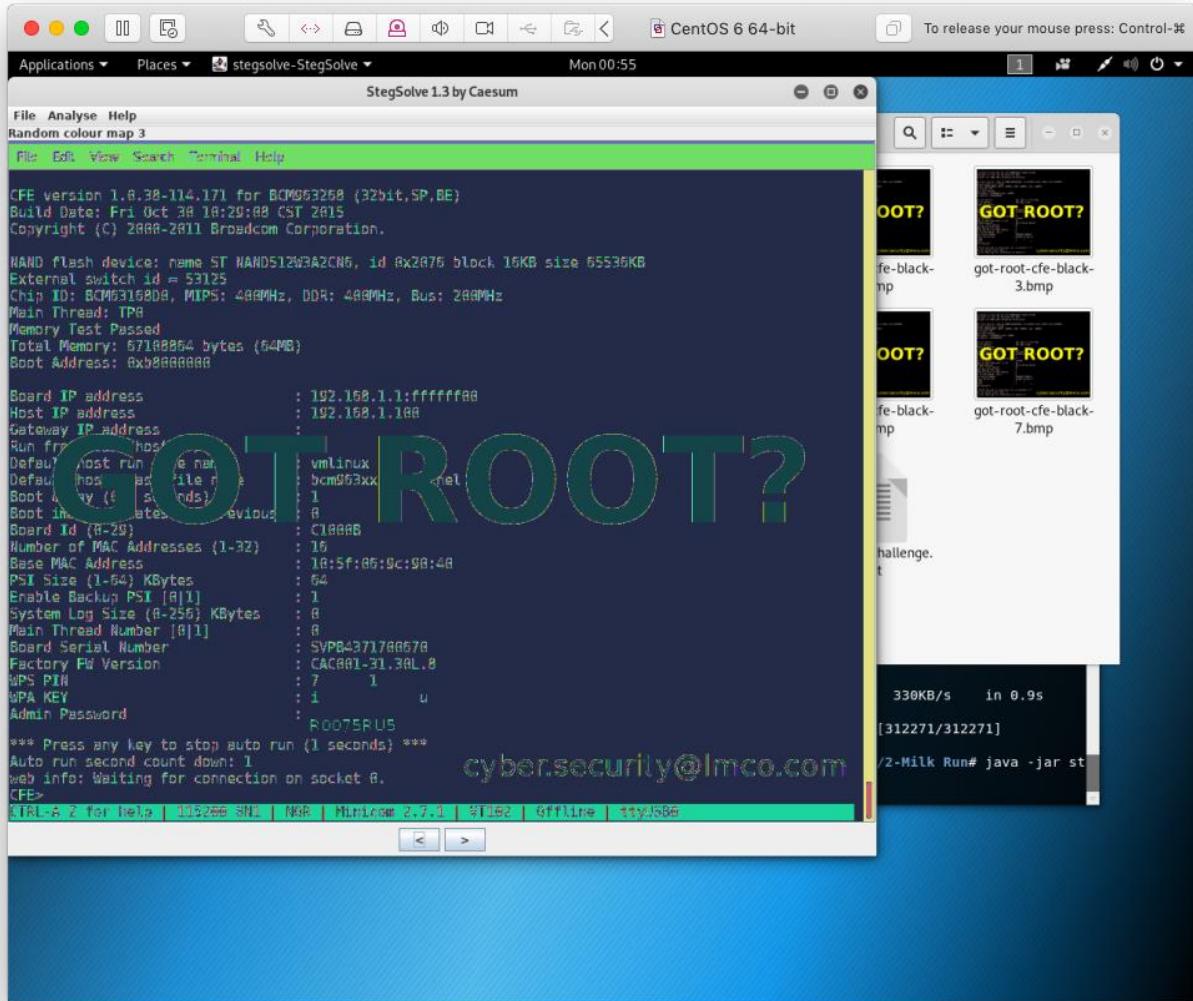


Level 3 – Got Root

Using StegSolve in Kali Linux, we were able to change color channel and expose the hidden flag for the particular image. The flag was hidden in the 6th file, and the password is: R0075RU5

See the screenshot below:





Level 4 – AI EDM

TAG Angel Cries Quickly

Opening with an hex editor, it uncovered the hidden flag at the end of the file

Program: OxED for Mac OS

Screenshot:

Level 5 – Final Frontier

Comment: nope

I uploaded the file on virustotal.com and then on the description tab on the page I scanned through the Exif data of the video file.

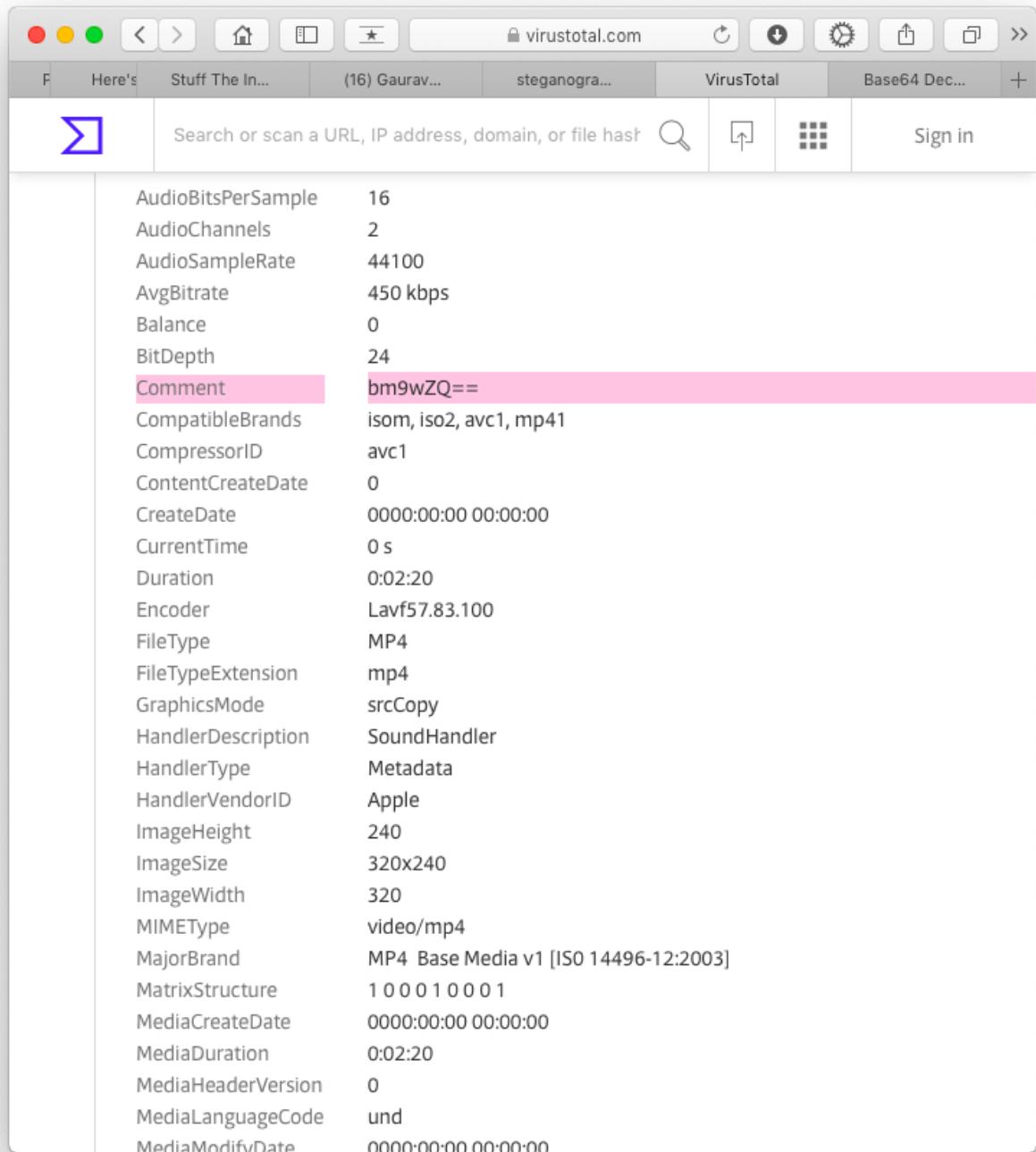
The Exif data of the file was extracted and we found base64 encoded string in one of the file attributes.

The video file has the comment parameter: "bm9wZQ==" which is a base64 encoded string text. The video file was scanned for any strings present in it but didn't yield much result except for some sting tokens. Kali Linux has forensic tools for digital forensics but not the best solution when it's a video file.

Any random characters that ends with == means it's a base64 encoded string and '=' characters are padded to the string to match its length.

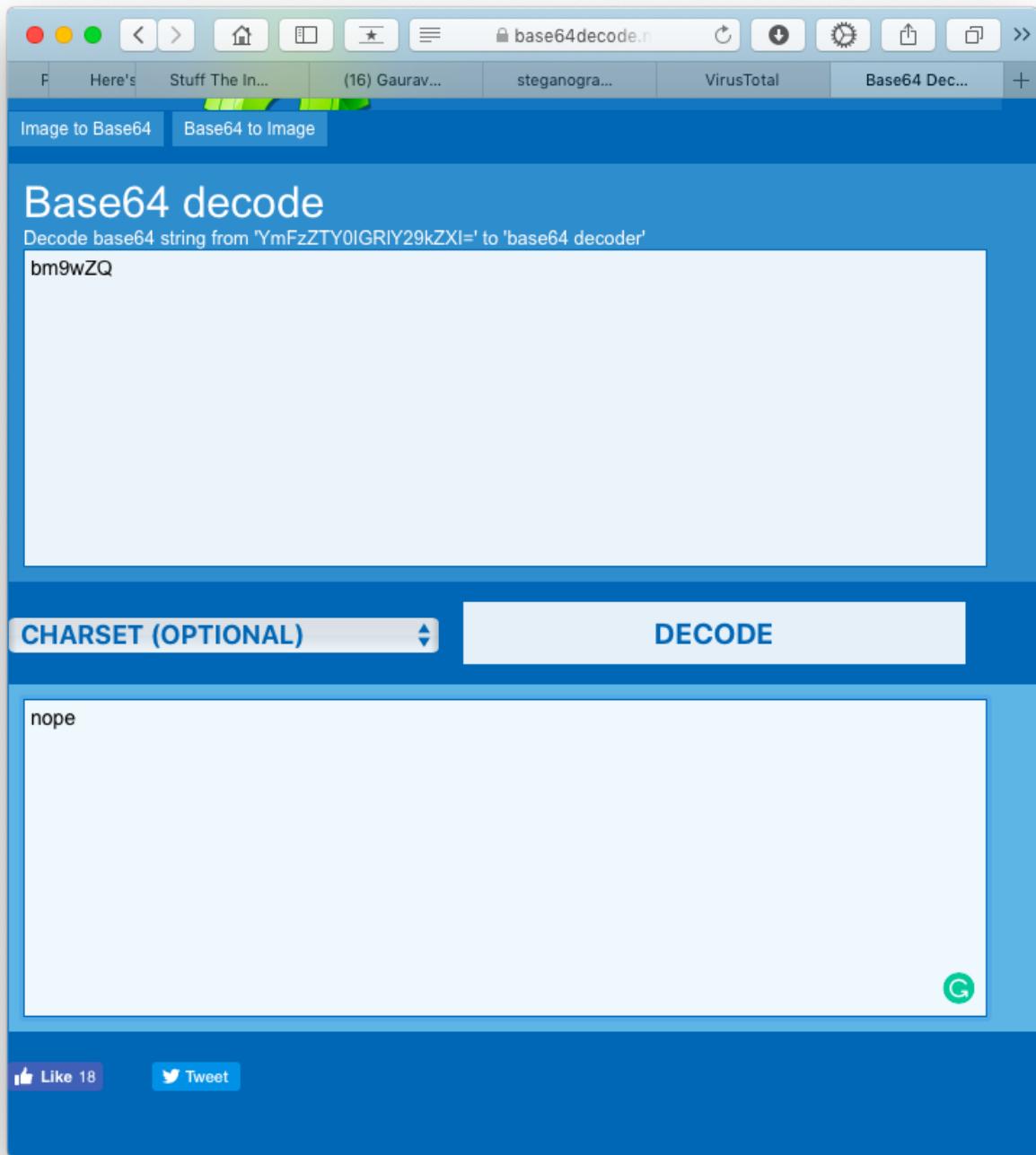
Thus on decoding the base64 string, it is: “nope”

Screenshot attached.



The screenshot shows a web browser window for virustotal.com. The address bar displays the URL. The main content area is a table of file metadata. A specific row, 'Comment', has a pink background highlight. The table includes columns for file properties and their corresponding values.

| | AudioBitsPerSample | 16 |
|--------------------|---------------------------------------|----|
| AudioChannels | 2 | |
| AudioSampleRate | 44100 | |
| AvgBitrate | 450 kbps | |
| Balance | 0 | |
| BitDepth | 24 | |
| Comment | bm9wZQ== | |
| CompatibleBrands | isom, iso2, avc1, mp41 | |
| CompressorID | avc1 | |
| ContentCreateDate | 0 | |
| CreateDate | 0000:00:00 00:00:00 | |
| CurrentTime | 0 s | |
| Duration | 0:02:20 | |
| Encoder | Lavf57.83.100 | |
| FileType | MP4 | |
| FileTypeExtension | mp4 | |
| GraphicsMode | srcCopy | |
| HandlerDescription | SoundHandler | |
| HandlerType | Metadata | |
| HandlerVendorID | Apple | |
| ImageHeight | 240 | |
| ImageSize | 320x240 | |
| ImageWidth | 320 | |
| MIMEType | video/mp4 | |
| MajorBrand | MP4 Base Media v1 [ISO 14496-12:2003] | |
| MatrixStructure | 1 0 0 1 0 0 0 1 | |
| MediaCreateDate | 0000:00:00 00:00:00 | |
| MediaDuration | 0:02:20 | |
| MediaHeaderVersion | 0 | |
| MediaLanguageCode | und | |
| MediaModifyDate | 0000:00:00 00:00:00 | |



Well, then it looks like Lockheed Martin isn't sending anyone back to the moon.