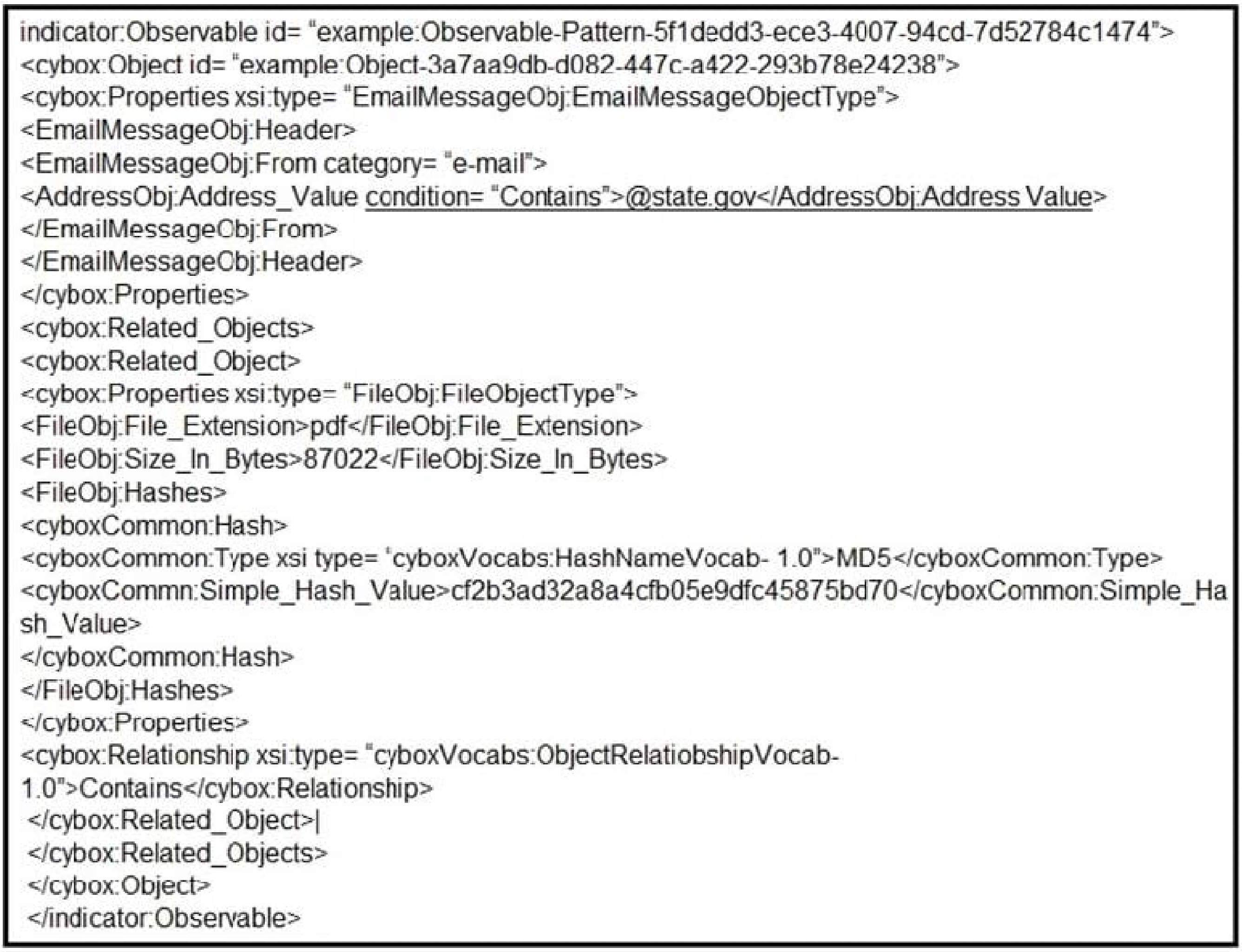
300-215 Q&As

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

QUESTION 1



```
indicator:Observable id= “example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474”>
<cybox:Object id= “example:Object-3a7aa9db-d082-447c-a422-293b78e24238”>
<cybox:Properties xsi:type= “EmailMessageObj:EmailMessageObjectType”>
<EmailMessageObj:Header>
<EmailMessageObj:From category= “e-mail”>
<AddressObj:Address_Value condition= “Contains”>@state.gov</AddressObj:Address_Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= “FileObj:FileObjectType”>
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= ‘cyboxVocabs:HashNameVocab- 1.0”>MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= “cyboxVocabs:ObjectRelatiobshipVocab-
1.0”>Contains</cybox:Relationship>
 </cybox:Related_Object>|
 </cybox:Related_Objects>
 </cybox:Object>
 </indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

B. Block all emails sent from an @state.gov address.

C. Block all emails with pdf attachments.

D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".

E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB

QUESTION 2

An engineer received a call to assist with an ongoing DDoS attack. The Apache server is being targeted, and availability is compromised. Which step should be taken to identify the origin of the threat?

A. An engineer should check the list of usernames currently logged in by running the command $ who | cut –d' ' -f1| sort | uniq

B. An engineer should check the server\\'s processes by running commands ps -aux and sudo ps -a.

C. An engineer should check the services on the machine by running the command service -status-all.

D. An engineer should check the last hundred entries of a web server with the command sudo tail -100 /var/log/apache2/access.log.

Correct Answer: D

QUESTION 3

What are YARA rules based upon?

A. binary patterns

B. HTML code

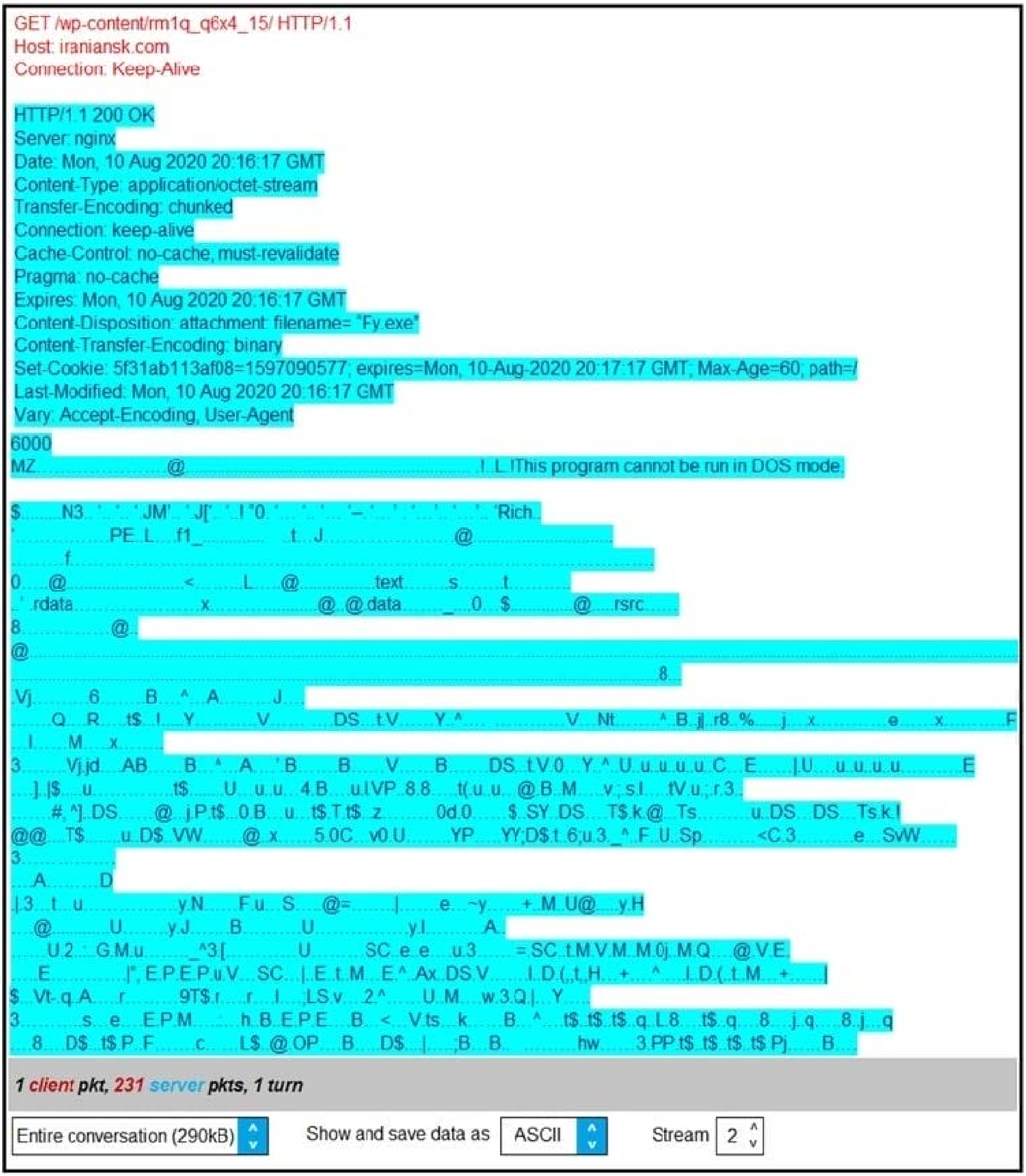
C. network artifacts

D. IP addresses

Correct Answer: A

Reference: https://en.wikipedia.org/wiki/YARA#:~:text=YARA%20is%20the%20name%20of,strings%20and%20a%20boolean%20expression.

QUESTION 4



```
GET /wp-content/rm1q_q6x4_15/ HTTP/1.1
Host: iraniansk.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Aug 2020 20:16:17 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 10 Aug 2020 20:16:17 GMT
Content-Disposition: attachment; filename="Fy.exe"
Content-Transfer-Encoding: binary
Set-Cookie: 5f31ab113af08=1597090577; expires=Mon, 10-Aug-2020 20:17:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 10 Aug 2020 20:16:17 GMT
Vary: Accept-Encoding, User-Agent
6000
MZ.....................@.......................................!..L.!This program cannot be run in DOS mode.

$.......N3..'..'..'JM'..'J['..'.!'0.'....'..'.....'—.'.....'..'.....'..'.....'..'Rich.
'.................PE..L....f1_..............t...J.......................@..........................
..........f...........................................................................................
0.....@.............................<..........L.....@...............text.........s.........t.........
_' .rdata............................x.........................@..@.data..........._.....0....$...........@.....rsrc.......
8..................@..
@..........................................................................................................................
.................................................................................................................8...
.Vj...........6.........B.....^....A.........J....
.........Q.....R.....t$..I.....Y...........V...........DS...t.V......Y.^....................V....Nt.........^.B.jj..r8..%.......j.....x.................e.........x...............F
....I.......M.....x.........
3..........Vj.jd....AB.........B....^.....A.....'B..........B..........V.........B..........DS..t.V.0....Y.^..U..u..u..u..u..C.....E.........|.U.....u..u..u..u...............E
.....]..|$.....u......................t$..........U.....u..u....4.B.....u.IVP..8.8.......t(.u..u...@.B..M.......v..;.s.I.......tV.u.;.r.3..
..........#,.^]..DS.........@...j.P.t$....0.B.....u.....t$.T.t$...z..............0d.0..........$..SY..DS.......T$.k.@....Ts.............u..DS.....DS.....Ts.k.!
@@.....T$..........u..D$..VW...........@..x..........5.0C.....v0.U.............YP.......YY;D$.t..6;u.3._^..F..U..Sp...............<C.3...............e....SvW.........
3.........................
.....A............D
.|.3....t....u..........................y.N..........F.u.....S........@=...........|...........e.....~y........+..M..U@.......y.H
.....@...................U..............y.J..........B...................U.....................................y.I...................A..
..........U.2...:..G.M.u..................^3.[..........................U..............SC..e..e.......u.3..............=.SC..t.M.V.M...M.0j..M.Q........@.V.E.
.......E.............................|",.E.P.E.P.u.V.....SC.....|..E..t..M......E.^..Ax.DS.V.............I..D.(.,t,.H.......+........^.........I..D.(..t..M.......+...........|
$....Vt-.q..A.........r......................9T$.r.......r.........I.........;LS.v........2.^..............U..M........w.3.Q.|......Y.........
3........................s.....e.......E.P.M................h..B..E.P.E.........B......<.....V.ts.......k..............B.......^.......t$..t$..t$...q..L.8.........t$..q........8..........j..q.........8..j.....q
.......8......D$.....t$.P..F.................c................L$..@.OP.........B............D$.....|............;B.....B......................hw..................3.PP.t$...t$...t$...t$.Pj...............B.......
```

1 client pkt, 231 server pkts, 1 turn

Entire conversation (290kB) Show and save data as ASCII Stream 2

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

A. Domain name:iraniansk.com

B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Content-Type: application/octet-stream

Correct Answer: CE

QUESTION 5

A security team received an alert of suspicious activity on a user\\'s Internet browser. The user\\'s anti-virus software indicated that the file attempted to create a fake recycle bin folder and connect to an external IP address. Which two actions should be taken by the security analyst with the executable file for further analysis? (Choose two.)

A. Evaluate the process activity in Cisco Umbrella.

B. Analyze the TCP/IP Streams in Cisco Secure Malware Analytics (Threat Grid).

C. Evaluate the behavioral indicators in Cisco Secure Malware Analytics (Threat Grid).

D. Analyze the Magic File type in Cisco Umbrella.

E. Network Exit Localization in Cisco Secure Malware Analytics (Threat Grid).

Correct Answer: BC