課題１：Drive-by Download 攻撃の時系列解析

特定 Web サイトの URL を 1 日ごとに半月の間、繰り返しアクセスした際の通信データを含んだ pcap ファイル（c101_20170815.pcap -- c101_20170831.pcap）と難読化された JavaScript を含んだ pcap ファイル（c102.pcap）とを解析して、以下の課題（１－１、１－２）に答えよ。

課題１－１

c101_20170815.pcap -- c101_20170831.pcap の中には、攻撃コードを含む pcap ファイルが 3 つ存在する。すなわち、同一 URL へのアクセスだとしても、攻撃コードを観測した日もあれば、観測しなかった日もあることを意味している。

課題１－１－１

c101_20170815.pcap -- c101_20170831.pcap を解析し、pcap ファイルに含まれる Web コンテンツの変化内容を以下の表 1 に沿って考え、表内の F-1 -- F-4 にあてはまる pcap ファイル名、および U1 -- U8 にあてはまる URL を回答せよ。

表 1. Drive-by Download 攻撃の時系列解析

pcap ファイル名	Web コンテンツの変化内容
（F-1）	（U-1）において（U-2）を参照する HTML タグが挿入され、また、（U-3）において使用されていた HTML タグの参照先 URL が、（U-4）から（U-2）へ変更された。 その結果、新しい参照先 URL（U-2）に含まれる（U-5）を参照する JavaScript が実行され、複数の URL へのアクセス後、最終的に攻撃コードを含む URL へのアクセスが**観測されるようになった。**
（F-2）	（U-2）にて使用されていた参照先 URL が、（U-5）から（U-6）へ変更された。参照先 URL が変更されたものの、（F-1）と同様の攻撃コードを含む URL へのアクセスが**観測された。**
（F-3）	（U-2）にて使用されていた参照先 URL が、（U-6）から（U-7）へ変更された。そのため、（F-1）および（F-2）で観測されていた攻撃コードを含む URL へのアクセスは**観測されなくなった。**
（F-4）	（U-2）にて使用されていた参照先 URL が、（U-7）から（U-8）へ変更された。その結果、（F-1）および（F-2）で観測されていた攻撃コードを含む URL へのアクセスが、再び**観測されるようになった。**しかし、翌日には（U-2）にて使用されていた参照先 URL が、再度（U-7）に変更され、以降攻撃コードを含む URL へのアクセスは**観測されなくなった。**

課題１－１－２

課題１−１−１にあるように、日ごとに攻撃コードを観測したり、もしくは観測しなかったりする原因として、c101_20170815.pcap -- c101_20170831.pcap から特定できる内容を、下記の選択肢の中からすべて答えよ。

【選択肢】

選択肢	原因
A	リダイレクト先 URL を変更する JavaScript が使用されたため。
B	入口 URL に該当する Web サイトの作成者（管理者）によって、攻撃コードを含む URL を参照するリダイレクトコードが削除されたため。
C	攻撃コードを含む Web コンテンツが削除されたため。
D	攻撃コードを含む URL のドメイン名が DNS 名前解決できなくなったため。
E	夏休みを終えた攻撃者がマルウェア感染活動に本気を出し始めたため。
F	攻撃コードを含む URL を参照するリダイレクトコードが変化したため。

課題１－２

c102.pcap の中には、難読化された JavaScript ファイルが 2 つ含まれる。
いずれかの JavaScript の難読化を解除し、難読化解除したコードに含まれる関数 generatePseudoRandomString() 内の変数 letters に代入される配列の最初（先頭）の値（すなわち、letters[0]）を答えよ。