

Capture The Flag (CTF)

Write Up LKS *CYBER SECURITY*



Tanggal, 10-11 Juni 2021

TEAM : CYBER SMKMUHDUPA

1	M. Rizki Akbar
2	Novran

Kategori Soal

Binary Exploitation/Pwn

PembandinganKata	200 Point
TimeMatters	300 Point
CanYouSeMe	500 Point
OverflowMe	500 Point

Reverse Engineering

Jawa	400 Point
Keygen	400 Point
Pyc	400 Point
Strcmp	400 Point

Cryptography

Caesar Cipher	500 Point
AES biasalah	200 Point
RSA Small e	200 Point
XOR	200 Point

Digital Forensic

Audiology	100 Point
Capture The Traffic	100 Point
Hidden Files	100 Point
Virus Program	400 Point

Web Exploitation

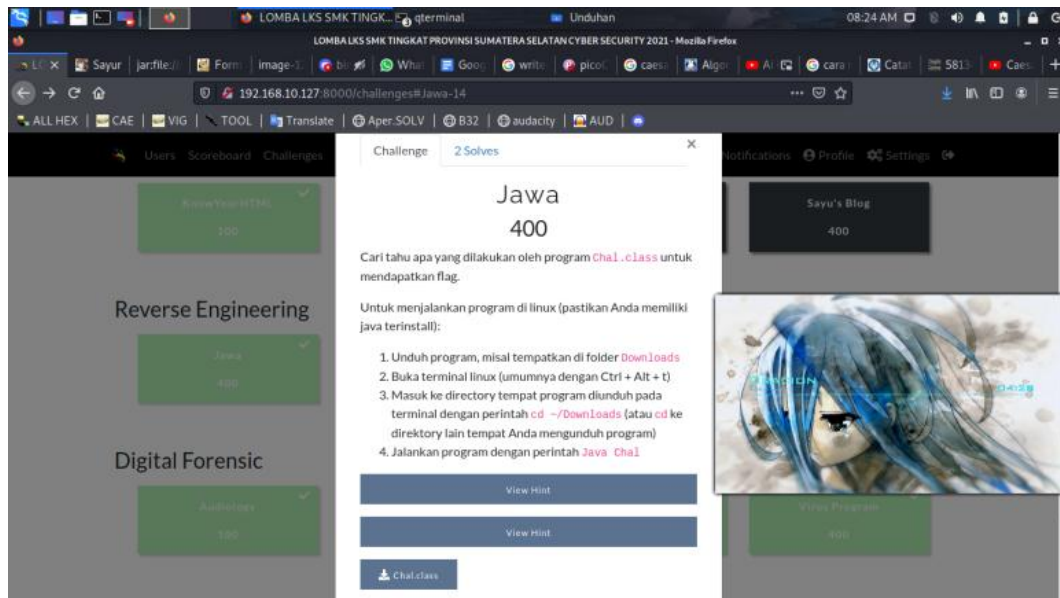
KnowYourHTML	100 Point
Invalid Browser	300 Point
Form Feedback	400 Point
Sayu's Blog	400 Point

Bonus

Reverse String	10 Point
-----------------------	-----------------

Reverse Engineering

Jawa 400 Point



Cara menyelesaikan:
Chal.class

```
Pattern pattern = Pattern.compile("LKSCS\\{.*\\}");
Matcher matcher = pattern.matcher(str1);
if (!matcher.matches()) {
    System.out.println("Harap masukkan input sesuai format flag LKSCS{<string>}");
    System.exit(1);
}
if (str1.length() != 30) {
    System.out.println("Panjang string harus 30");
    System.exit(1);
}
String str2 = str1.substring(6, 29);
if (str2.charAt(7) != '_') {
    System.out.println("Input salah 1 ");
    System.exit(1);
}
if (str2.charAt(14) != '_') {
    System.out.println("Input salah 2 ");
    System.exit(1);
}
if (str2.charAt(19) != '_') {
    System.out.println("Input salah 3 ");
    System.exit(1);
}
String[] arrayOfString = str2.split("_", 0);
```

```

    if (!arrayOfString[0].equals("belajar")) {
        System.out.println("Input salah 4 ");
        System.exit(1);
    }
    if (!(new
StringBuilder(arrayOfString[1])).reverse().toString().equals("asahab"))
{
        System.out.println("Input salah 5 ");
        System.exit(1);
    }
    if (!arrayOfString[2].equals("jawa")) {
        System.out.println("Input salah 6 ");
        System.exit(1);
    }
    if (!(new
StringBuilder(arrayOfString[3])).reverse().toString().equals("hig")) {
        System.out.println("Input salah 7 ");
        System.exit(1);
    }

```

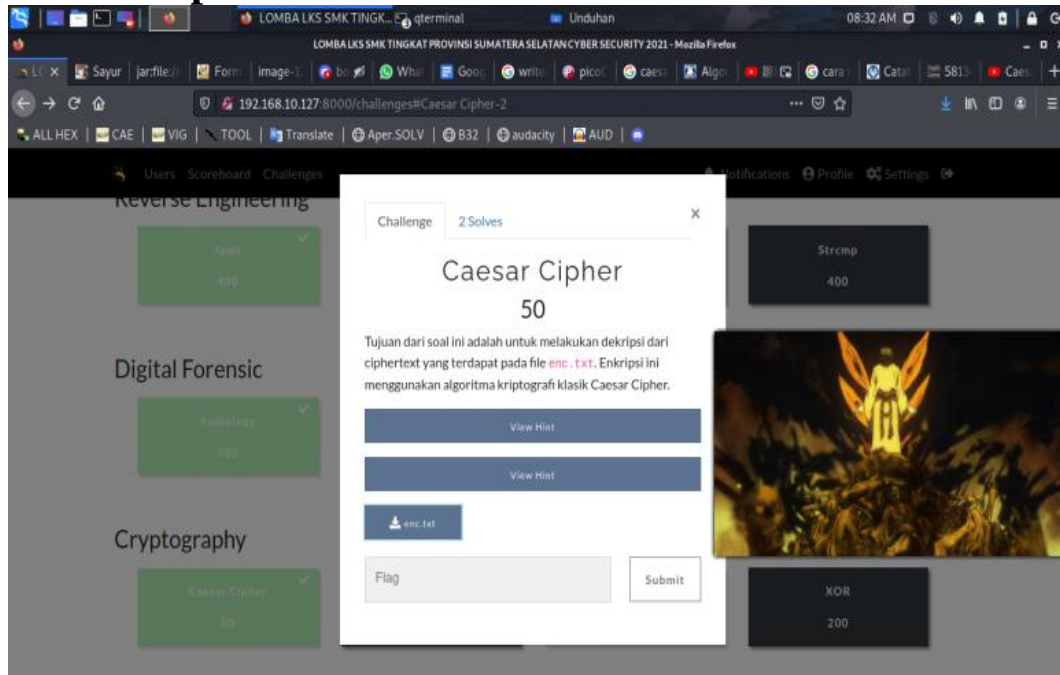
Dari potongan script diatas diatas, bisa disimpulkan bahwa :

- Format flag sudah diberikan yaitu LKSCS{
- Kata berikutnya terdapat di baris ke-40 dimana ada ada fungsi untuk mengambil array pertama yaitu **belajar**
- Selanjutnya pada baris ke-45 terdapat string **asahab** yang jika di reverse (karena sudah ada fungsi reverse() yang hasilnya menjadi **Bahasa**
- Array ketiga adalah **jawa**
- Terdapat fungsi reverse() pada baris ke-55 yang menandakan teks nya adalah **gih**.
- Setiap kata diberikan garisbawah (_) sebagai pemisah/pengganti spasi
- Maka dapat disimpulkan hasilnya adalah **belajar_bahasa_jawa_gih** dan flag nya adalah **LKSCS{belajar_bahasa_jawa_gih}**

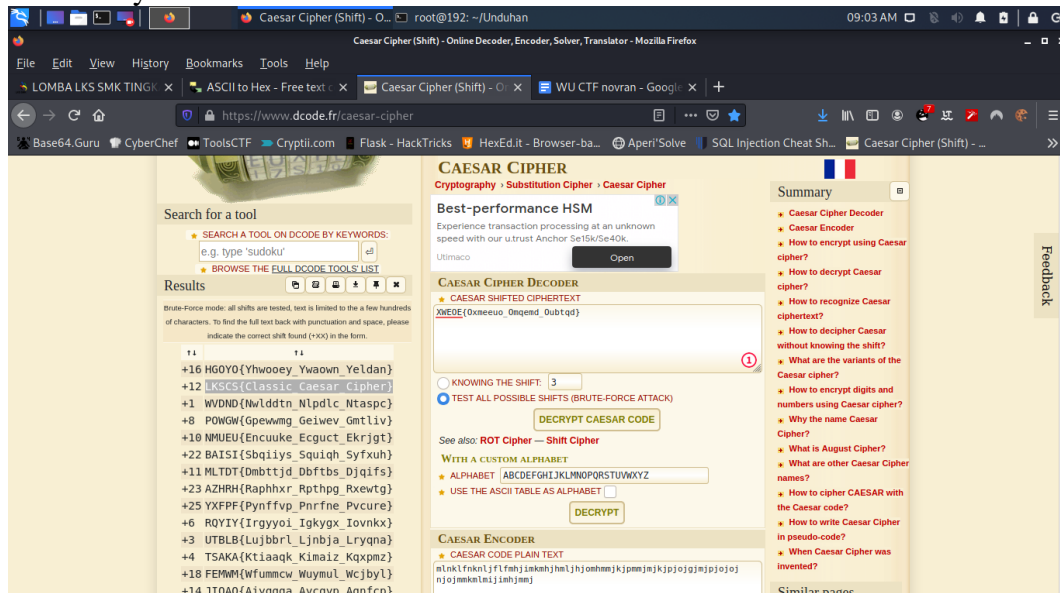
FLAG : LKSCS{belajar_bahasa_jawa_gih}

Cryptography

Caesar Cipher



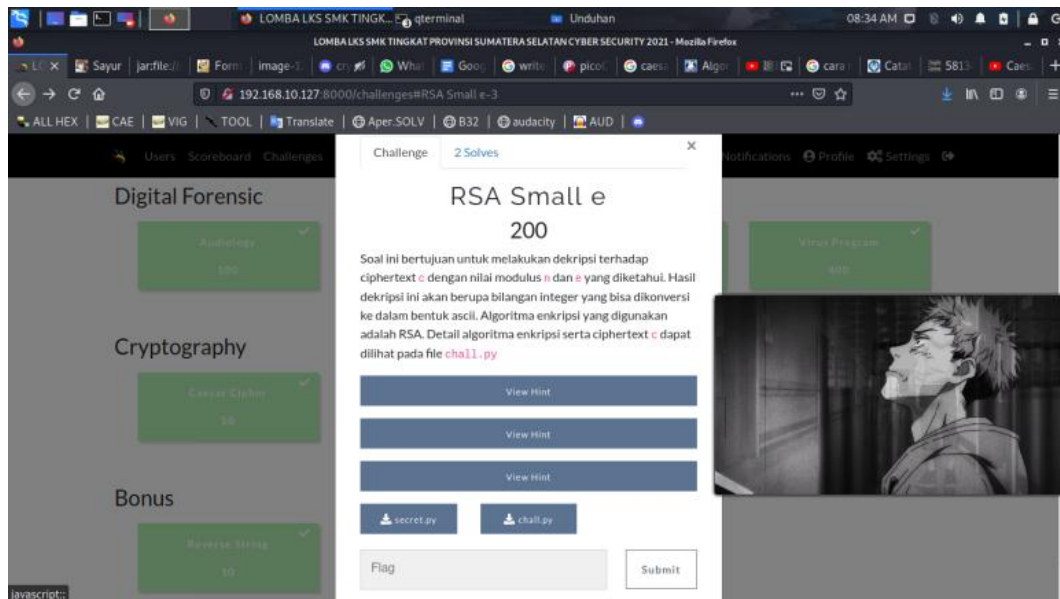
Cara menyelesaikan:



Menggunakan <https://www.dcode.fr/caesar-cipher> lalu ngebruteforce key untuk mendapatkan Flag

FLAG : LKSCS{Classic_Caesar_Cipher}

RSA Small e



Cara menyelesaikan:

Diberikan script python3 sebagai berikut

```
#!/usr/bin/python3
from Crypto.Util.number import *
from secret import flag

m = bytes_to_long(flag)
e = 3
p = getRandomNBitInteger(512)
q = getRandomNBitInteger(512)
n = p*q

c = pow(m, e, n)
print("n : {0}".format(n))
print("c : {0}".format(c))
# n :
145617125671053637155694053597315277961712528432487711571135593053
636759388923038405490228028803146311152135181934446049719093297743
066773782935675794466099044256928735050655622320924024284199287256
967546582443495371350496323071174039030864993944794254395751096165
557723969120034490038893742824286837390573140
# c :
194067004507066782053628916063324736362917479205341092387170757780
095970447997003853504461502945860113357537528451415300004597585951
809209940303462403230502192711983655990551751381158185667678488867
716576067973799378823680434723967647764675602501601637
```

Diketahui nilai **exponent** nya adalah **e = 3**, **ciphertext** yang dikonversi menjadi bilangan decimal yaitu **c =**

194067004507066782053628916063324736362917479205341092387170757780
095970447997003853504461502945860113357537528451415300004597585951
809209940303462403230502192711983655990551751381158185667678488867
716576067973799378823680434723967647764675602501601637 , nilai modulus
adalah $n =$
145617125671053637155694053597315277961712528432487711571135593053
636759388923038405490228028803146311152135181934446049719093297743
066773782935675794466099044256928735050655622320924024284199287256
967546582443495371350496323071174039030864993944794254395751096165
557723969120034490038893742824286837390573140 . Biasanya diperlukan
bilangan prima dari p dan q dimana p dan q adalah perkalian yang menghasilkan nilai
modulus (n). Menggunakan situs <https://factordb.com> untuk melakukan faktorisasi nilai
n tersebut namun tidak mendapatkan titik terang

←	→	↻	🔍	factordb.com/index.php?query=145617125671053637155694053597315277961712528432487711571135593053636759388923038405490228028803146311152135181934446049719093297743066773782935675794466099044256928735050655622320924024284199287256967546582443495371350496323071174039030864993944794254395751096165557723969120034490038893742824286837390573140	
Search	Sequences	Report results	Factor tables	Status	Downloads
145617125671053637155694053597315277961712528432487711571135593053636759388923038405490228028803146311152135181934446049719093297743066773782935675794466099044256928735050655622320924024284199287256967546582443495371350496323071174039030864993944794254395751096165557723969120034490038893742824286837390573140 Factorize!					
Result:					
status (?)	digits	number			
CF	309 (show)	1456171256_40<309> = 2^2 · 3^3 · 5 · 71 · 557 · 33601 · 90448913 · 2243621515_81<289>			

<http://factordb.com/index.php?query=145617125671053637155694053597315277961712528432487711571135593053636759388923038405490228028803146311152135181934446049719093297743066773782935675794466099044256928735050655622320924024284199287256967546582443495371350496323071174039030864993944794254395751096165557723969120034490038893742824286837390573140>

Karena nilai exponent nya kecil (low exponent), maka bisa menggunakan script berikut ini untuk mendapatkan flagnya

```
import sys
n=
222721290805627228866140226322054427054944552728601128140930835000
977233668976511610291021788064683648105601453266742989437489263120
593193331040248776294143550819975111705718417265548703304384491364
149427698794499099452806226799824169615052596057487005276260641763
454283480756666189664133580666747662446021203344059190540450974650
421778275667620566124975394033923711742596028546499571615826161106
653587742099544832438078932250115116700258508007171825355755778485
005274302462591340719809799518035998632107050041347640271269838388
845187042396829648976190300917890476305568076454114170771496175598
60988186649846538955623
n=hex(n)
e=3
cipher=
562749201081224789908880925213717396055139590533222622291387717236
540331677561281220862297224061805931286646965129123115753277247246
95863345048713415525599333
```

```

import gmpy2

with gmpy2.local_context(gmpy2.context(), precision=800) as ctx:
    ctx.precision += 800
    root = gmpy2.cbrt(cipher)

try:
    print(str('%x' % int(root)).decode('hex'))
except AttributeError:
    print(bytes.fromhex(str('%x' % int(root))).decode('utf-8'))

```

```

L- cat rsa.py 66 echo "\n" 66 python3 rsa.py
import sys
n= 1456171256710536371556940535973152779617125284224877115711355930536367593889230384054902280288031463111521351819344460497190932977420667737829356757944660990442569287
35050655622328924024284199287256967546582443495371359496323071174039030864993944794254395751096165557723969120034490038893742824286837390573140
n=hex(n)
e=3
cipher= 19406780450706678205362891606322473636291747920534109238717075778009597044799700385350446150294586011335753752845141530000459758595180920994030346240323850219271
1983655990551751381158185667678488867716576067973799378823680434723967647764675602501601637
import gmpy2

with gmpy2.local_context(gmpy2.context(), precision=800) as ctx:
    ctx.precision += 800
    root = gmpy2.cbrt(cipher)

try:
    print(str('%x' % int(root)).decode('hex'))
except AttributeError:
    print(bytes.fromhex(str('%x' % int(root))).decode('utf-8'))

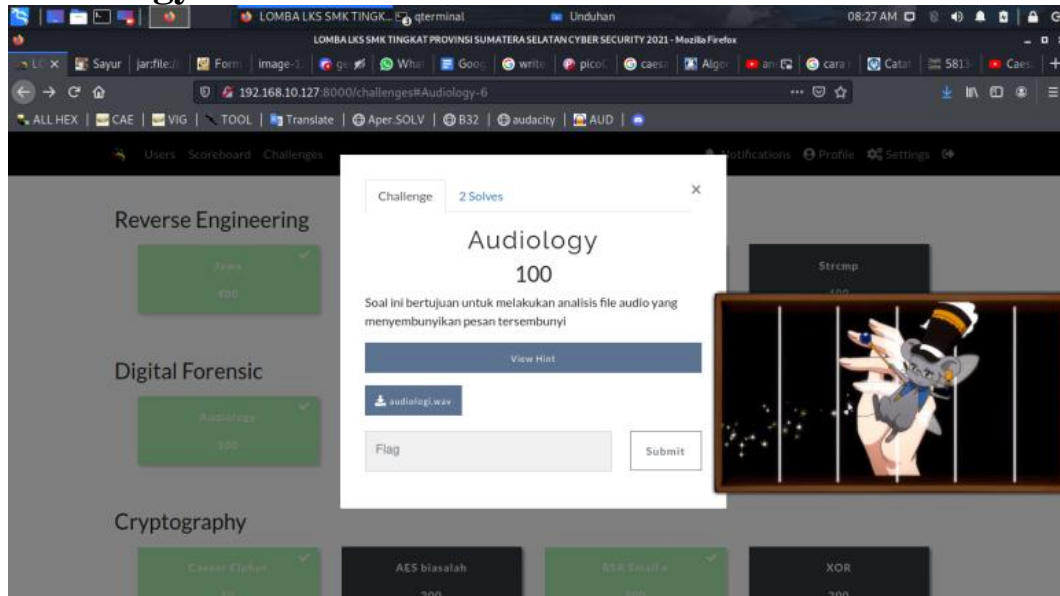
LKSCS{RSA_attack_on_small_exponent}

```

Flag : LKSCS{RSA_attack_on_small_exponent}

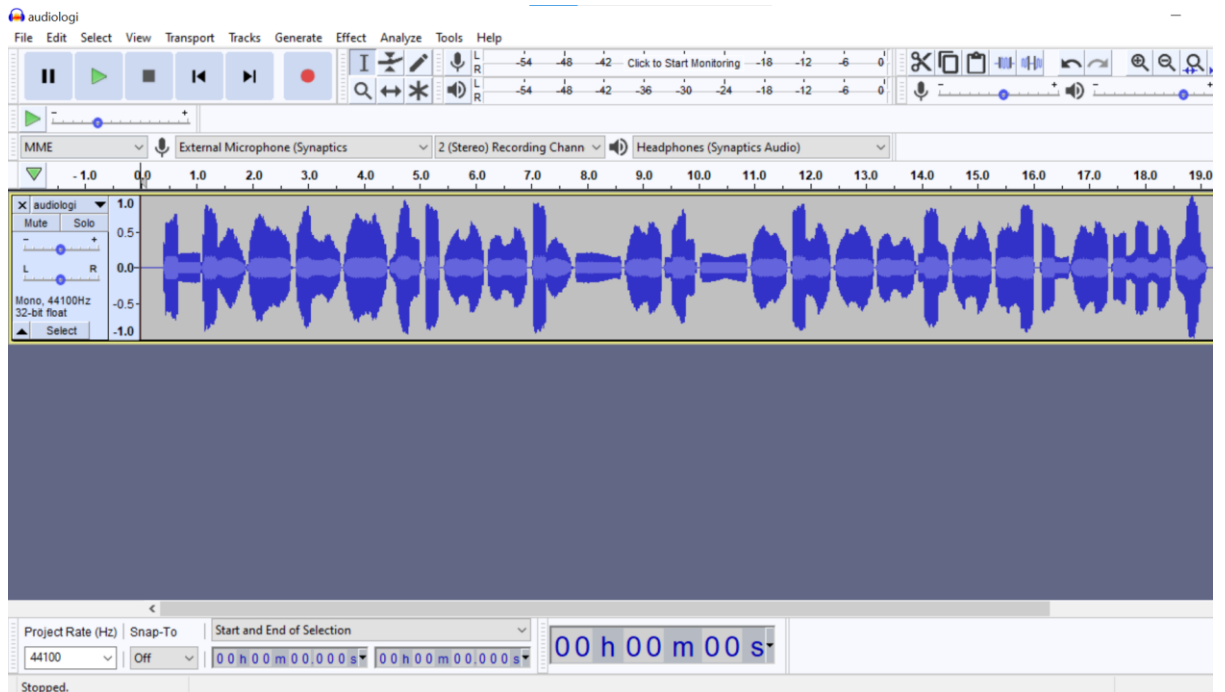
Digital Forensic

Audiology

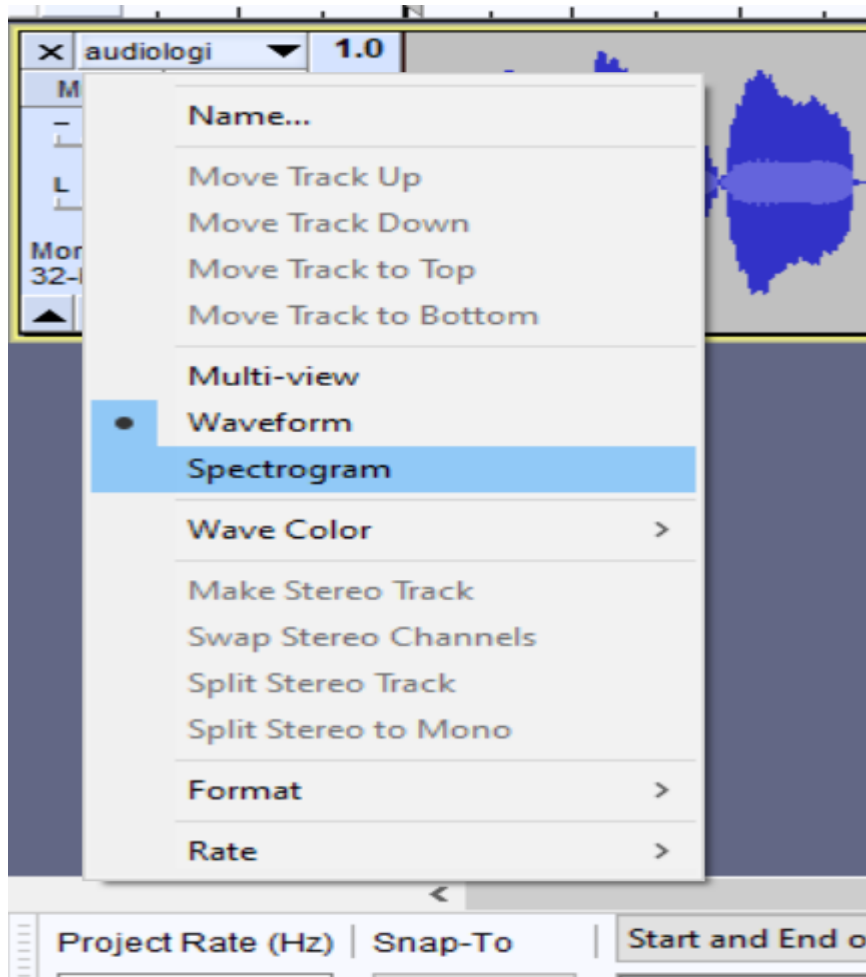


Cara menyelesaikan:

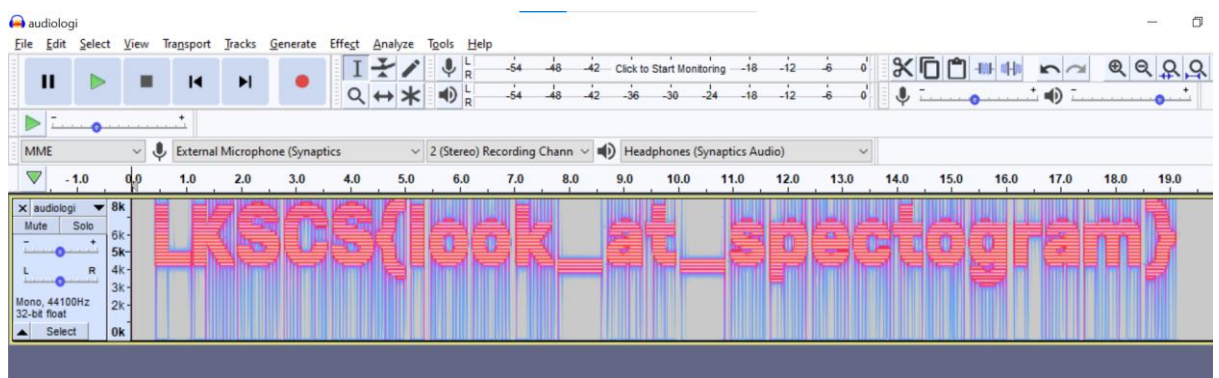
Buka file audiologi.wav menggunakan Audacity



Ubah View dari Waveform menjadi Spectrogram

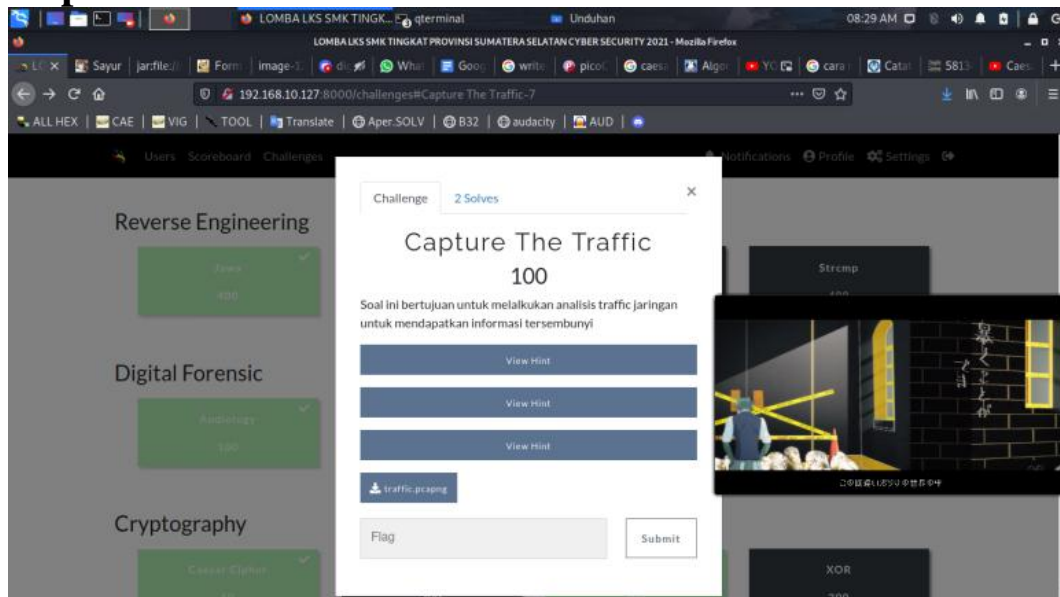


Flag terlihat



FLAG : LKSCS{look_at_spectrogram}

Capture The Traffic



Cara menyelesaikan:
Buka file traffic.png menggunakan Wireshark

traffic.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	sc-in-F94.1e100...	192.168.98.134	UDP	67	443 → 63092 Len=25
2	0.366092	192.168.98.134	104.21.15.37	TCP	55	54315 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1 [TCP segment of a reassembled PDU]
3	0.446682	104.21.15.37	192.168.98.134	TCP	54	443 → 54315 [ACK] Seq=1 Ack=2 Win=13364 Len=0
4	0.592298	ee:48:c5:a2:d4:e0	Tp-LinkT_d7:d9:43	ARP	42	Who has 192.168.98.134? Tell 192.168.98.53
5	0.592325	Tp-LinkT_d7:d9:43	ee:48:c5:a2:d4:e0	ARP	42	192.168.98.134 is at 84:16:f9:d7:d9:43
6	1.608503	117.18.237.29	192.168.98.134	TCP	54	80 → 65094 [ACK] Seq=1 Ack=1 Win=65535 Len=0
7	1.608550	192.168.98.134	117.18.237.29	TCP	54	[TCP ACKed unseen segment] 65094 → 80 [ACK] Seq=1 Ack=2 Win=65280 Len=0
8	2.935052	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who has 192.168.98.101? Tell 192.168.98.53
9	3.835592	192.168.98.134	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
10	3.959032	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who has 192.168.98.101? Tell 192.168.98.53
11	4.000628	fe80::17d:5b0b:c...	ff02::c	UDP	1154	64085 → 3702 Len=1092
12	4.000661	192.168.98.134	239.255.255.250	UDP	1122	64084 → 3702 Len=1080
13	4.077847	fe80::17d:5b0b:c...	ff02::c	UDP	1154	64085 → 3702 Len=1092
14	4.093454	192.168.98.134	239.255.255.250	UDP	1122	64084 → 3702 Len=1080
15	4.210962	fe80::17d:5b0b:c...	ff02::c	UDP	1154	64085 → 3702 Len=1092
16	4.281604	192.168.98.134	239.255.255.250	UDP	1122	64084 → 3702 Len=1080
17	4.486142	fe80::17d:5b0b:c...	ff02::c	UDP	1154	64085 → 3702 Len=1092
18	4.641873	192.168.98.134	239.255.255.250	UDP	1122	64084 → 3702 Len=1080
19	4.983081	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who has 192.168.98.101? Tell 192.168.98.53
20	5.108997	192.168.98.134	192.168.98.246	TCP	54	63321 → 5000 [FIN, ACK] Seq=1 Ack=1 Win=256 Len=0
21	5.109013	192.168.98.134	192.168.98.246	TCP	66	51346 → 5000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	5.191161	192.168.98.246	192.168.98.134	TCP	54	5000 → 63321 [ACK] Seq=1 Ack=2 Win=4096 Len=0
23	5.191161	192.168.98.246	192.168.98.134	TCP	66	5000 → 51346 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 SACK_PERM=1
24	5.191452	192.168.98.134	192.168.98.246	TCP	54	51346 → 5000 [ACK] Seq=1 Ack=1 Win=65536 Len=0
25	5.193100	192.168.98.134	192.168.98.246	HTTP	193	GET / HTTP/1.1
26	5.196822	192.168.98.246	192.168.98.134	TCP	54	[TCP Window Update] 5000 → 51346 [ACK] Seq=1 Ack=1 Win=262144 Len=0
27	5.197399	192.168.98.246	192.168.98.134	TCP	54	5000 → 51346 [ACK] Seq=1 Ack=140 Win=261952 Len=0
28	5.200245	192.168.98.246	192.168.98.134	TCP	1514	5000 → 51346 [ACK] Seq=1 Ack=140 Win=262144 Len=1408 [TCP segment of a reassembled PDU]
29	5.200245	192.168.98.246	192.168.98.134	HTTP	88	HTTP/1.1 200 OK (text/html)
30	5.200412	192.168.98.134	192.168.98.246	TCP	54	51346 → 5000 [ACK] Seq=140 Ack=1495 Win=65536 Len=0
31	5.509624	192.168.98.134	192.168.98.53	DNS	77	Standard query 0x943c A beacon4.gvt2.com
32	5.608122	192.168.98.53	192.168.98.134	DNS	93	Standard query response 0x943c A beacon4.gvt2.com A 216.239.32.116
33	5.662279	192.168.98.134	beacon4.gvt2.com	QUIC	1392	Initial, DCID=2cc9b59c625d2e73, PKN: 1, CRYPTO, PADDING
34	5.834366	beacon4.gvt2.com	192.168.98.134	QUIC	1392	Protected Payload (KP0)
35	5.835614	192.168.98.134	beacon4.gvt2.com	QUIC	281	Protected Payload (KP0), DCID=2cc9b59c625d2e73
36	5.835956	192.168.98.134	beacon4.gvt2.com	QUIC	382	Protected Payload (KP0), DCID=2cc9b59c625d2e73
37	5.940414	beacon4.gvt2.com	192.168.98.134	QUIC	670	Protected Payload (KP0)
38	5.940414	beacon4.gvt2.com	192.168.98.134	QUIC	119	Protected Payload (KP0)
39	5.941124	192.168.98.134	beacon4.gvt2.com	QUIC	75	Protected Payload (KP0), DCID=2cc9b59c625d2e73
40	5.965835	beacon4.gvt2.com	192.168.98.134	QUIC	69	Protected Payload (KP0)
41	5.965835	beacon4.gvt2.com	192.168.98.134	QUIC	67	Protected Payload (KP0)
42	5.965835	beacon4.gvt2.com	192.168.98.134	QUIC	380	Protected Payload (KP0)

Terdapat beberapa protocol seperti TCP, HTTP, UDP, ARP, dll. Fokus kami adalah protocol HTTP karna isi dari frame nya bisa dilihat dengan jelas dan tidak terenkripsi seperti HTTPS.

Klik kanan Frame protocol TCP, pilih Follow -> TCP Stream

The screenshot shows the Wireshark interface with a packet list on the left and a context menu open over a selected TCP packet (No. 20). The packet list shows various protocols including UDP, TCP, ARP, and HTTP. The context menu includes options like 'Follow', 'Copy', 'Protocol Preferences', and 'Decode As...'. The 'Follow' option is highlighted, and a submenu is visible showing 'TCP Stream', 'UDP Stream', 'TLS Stream', 'HTTP Stream', 'HTTP/2 Stream', and 'QUIC Stream'. The 'TCP Stream' option is selected, and its keyboard shortcut 'Ctrl+Alt+Shift+T' is displayed.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	sc-in-f94.1e100...	192.168.98.134	UDP	67	443 → 63092 Len=25
2	0.366092	192.168.98.134	104.21.15.37	TCP	55	[54] → 80 Len=0
3	0.446682	104.21.15.37	192.168.98.134	TCP	54	80 → [54] Len=0
4	0.592298	ee:48:c5:a2:d4:e0	tp-link_t_d7:d9:43	ARP	42	Who's on the network?
5	0.592325	tp-link_t_d7:d9:43	ee:48:c5:a2:d4:e0	ARP	42	Who's on the network?
6	1.608503	117.18.237.29	192.168.98.134	TCP	54	80 → [54] Len=0
7	1.608550	192.168.98.134	117.18.237.29	TCP	54	[54] → 80 Len=0
8	2.935052	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who's on the network?
9	3.833592	192.168.98.134	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
10	3.959032	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who's on the network?
11	4.000628	fe80::17d:5b00:c...	ff02::c	UDP	1154	644
12	4.000861	192.168.98.134	239.255.255.250	UDP	1122	644
13	4.077847	fe80::17d:5b00:c...	ff02::c	UDP	1154	644
14	4.093454	192.168.98.134	239.255.255.250	UDP	1122	644
15	4.219062	fe80::17d:5b00:c...	ff02::c	UDP	1154	644
16	4.281604	192.168.98.134	239.255.255.250	UDP	1122	644
17	4.486142	fe80::17d:5b00:c...	ff02::c	UDP	1154	644
18	4.641873	192.168.98.134	239.255.255.250	UDP	1122	644
19	4.983081	ee:48:c5:a2:d4:e0	Broadcast	ARP	42	Who's on the network?
20	5.108997	192.168.98.134	192.168.98.246	TCP	54	63
21	5.109013	192.168.98.134	192.168.98.246	TCP	66	51
22	5.191161	192.168.98.246	192.168.98.134	TCP	54	50
23	5.191161	192.168.98.246	192.168.98.134	TCP	66	50
24	5.191452	192.168.98.134	192.168.98.246	TCP	54	51
25	5.193100	192.168.98.134	192.168.98.246	HTTP	193	GET / HTTP/1.1
26	5.196822	192.168.98.246	192.168.98.134	TCP	54	51
27	5.197399	192.168.98.246	192.168.98.134	TCP	54	50
28	5.200245	192.168.98.246	192.168.98.134	TCP	1514	5000 → 51346 [ACK] Seq=140 Win=262144 Len=146
29	5.200245	192.168.98.246	192.168.98.134	HTTP	88	HTTP/1.1 200 OK (text/html)
30	5.200412	192.168.98.134	192.168.98.246	TCP	54	51346 → 5000 [ACK] Seq=140 Ack=1495 Win=65536 Len=0
31	5.509624	192.168.98.134	192.168.98.53	DNS	77	Standard query 0x943c A beacons4.gvt2.com
32	5.660122	192.168.98.53	192.168.98.134	DNS	93	Standard query response 0x943c A beacons4.gvt2.com A 216.239.32.116
33	5.662279	192.168.98.134	beacons4.gvt2.com	QUIC	1392	Initial, DCID=2cc9b59c625d2e73, PKN: 1, CRYPTO, PADDING
34	5.834366	beacons4.gvt2.com	192.168.98.134	QUIC	1392	Protected Payload (KPB)
35	5.835614	192.168.98.134	beacons4.gvt2.com	QUIC	201	Protected Payload (KPB), DCID=2cc9b59c625d2e73
36	5.835956	192.168.98.134	beacons4.gvt2.com	QUIC	302	Protected Payload (KPB), DCID=2cc9b59c625d2e73
37	5.940414	beacons4.gvt2.com	192.168.98.134	QUIC	670	Protected Payload (KPB)
38	5.940414	beacons4.gvt2.com	192.168.98.134	QUIC	119	Protected Payload (KPB)
39	5.941124	192.168.98.134	beacons4.gvt2.com	QUIC	75	Protected Payload (KPB), DCID=2cc9b59c625d2e73
40	5.965035	beacons4.gvt2.com	192.168.98.134	QUIC	69	Protected Payload (KPB)
41	5.965035	beacons4.gvt2.com	192.168.98.134	QUIC	67	Protected Payload (KPB)
42	5.965236	beacons4.gvt2.com	192.168.98.134	QUIC	389	Protected Payload (KPB)

Pada stream ketiga, terdapat teks dengan format Flag LKSCS{

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.906
Host: 192.168.98.246:5000

HTTP/1.1 200 OK
Content-Length: 1182
Content-Disposition: inline; filename="index.html"
Accept-Ranges: bytes
ETag: "d91703c91612a9db082ab7033278e56d3a905b1f"
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Fri, 04 Jun 2021 15:16:17 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<!DOCTYPE html>
<html>
<title>FLAG</title>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway">
<style>
  body,h1 {font-family: "Raleway", sans-serif}
  body, html {height: 100%}
  .bgimg {
    background-image: url('https://www.w3schools.com/w3images/forestbridge.jpg');
    min-height: 100%;
    background-position: center;
    background-size: cover;
  }
</style>
<body>

<div class="bgimg w3-display-container w3-animate-opacity w3-text-white">
  <div class="w3-display-topleft w3-padding-large w3-xlarge">
    Logo
  </div>
  <div class="w3-display-middle">
    <h1 class="w3-jumbo w3-animate-top">LKSCS{3xp0rt_7r4ffic_0Bjec7}</h1>
    <hr class="w3-border-grey" style="margin:auto;width:40%">
    <p class="w3-large w3-center">FLAG</p>
  </div>
  <div class="w3-display-bottomleft w3-padding-large">
    Powered by <a href="https://www.w3schools.com/w3css/default.asp" target="_blank">w3.css</a>
  </div>
</div>

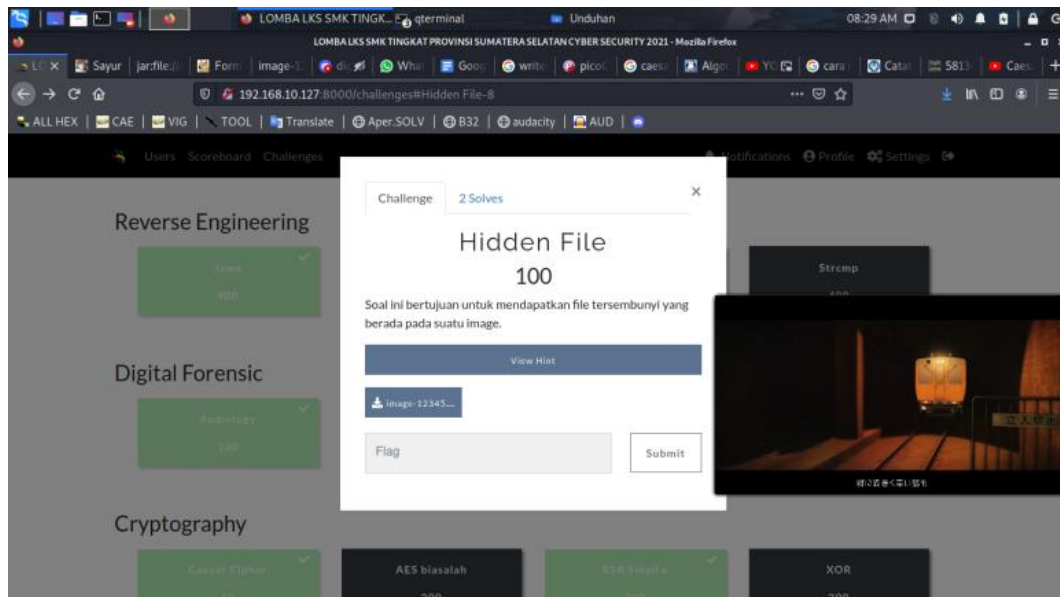
</body>
</html>

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.906
Host: 192.168.98.246:5000

HTTP/1.1 200 OK
Content-Length: 1182
Content-Disposition: inline; filename="index.html"
Accept-Ranges: bytes
```

FLAG : LKSCS{3xp0rt_7r4ffic_0Bjec7}

Hidden Files



Cara menyelesaikan:

dikasih file gambar dengan ekstensi .png. Menggunakan commands strings untuk mendapatkan flag.

```
strings image-12345.png
```

```
-----
```

```
flag.txtLKSCS{UnZ1p_th3_lm4g3}PK
```

```
flag.txt
```

```
-----
```

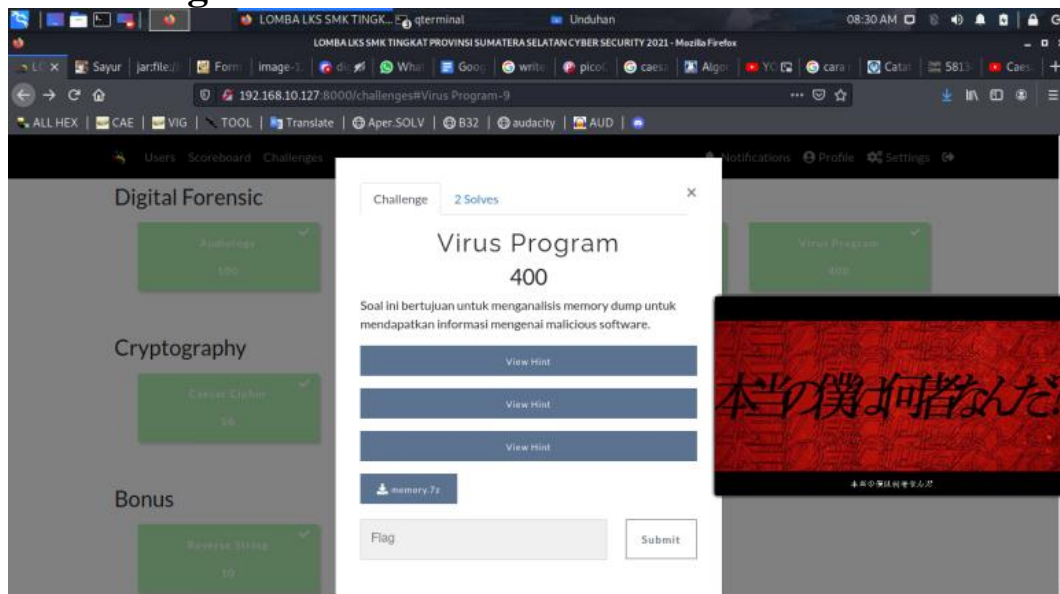
```

@ E~
zGp7
:M-
T6e"
s,FN97c=o
wk'@
p:S.
Y-;}X
k^70
I1i[
0-J\ ' )
&\uh"
SJ2zvG
'T_9
"ldo
, AC
o6ge
@`nkAnd
V_FCS
^IDAT
b7{F
@/3v
1t(A
#DT0
i#&"
K=]xL
\dWP
}F:Y
IEND
flag.txtLKSCS{UnZ1p_th3_Im4g3}PK
flag.txt

```

FLAG : LKSCS{UnZ1p_th3_Im4g3}

Virus Program



Cara menyelesaikan:

Diberikan file Bernama memory.dmp. Setelah di cek menggunakan command **file**, diketahui bahwa file tersebut merupakan dump dari suatu memory komputer

```
L# file memory.dmp
memory.dmp: MS Windows 32bit crash dump, no PAE, full dump, 130958 pages
```

Ada dua cara untuk mendapatkan flag, pertama menggunakan command strings dan yang kedua menggunakan volaitlity

Cara pertama :

strings memory.dmp | grep LKSCS{

```
L# strings memory.dmp | grep LKSCS{
LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
LKSCS{H1dd3n_Pr06r4m!!!}.exe
sLKSCS{H1dd3n_Pr06r4m!!!}
bLKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
LKSCS{-1.EXE
opiy-windows-manifest-filename LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
LKSCS{H1dd3n_Pr06r4m!!!}
LKSCS{H1dd3n_P
LKSCS{H1dd3n_P
LKSCS{H1dd3n_Pr06r4m!!!}.exe
sLKSCS{H1dd3n_Pr06r4m!!!}
bLKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
opiy-windows-manifest-filename LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
opiy-windows-manifest-filename LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
C:\LKSCS{H1dd3n_Pr06r4m!!!}.pkg
LKSCS{H1dd3n_P
<assemblyIdentity type="win32" name="LKSCS{H1dd3n_Pr06r4m!!!}" processorArchitecture="x86" version="1.0.0.0"/>
LKSCS{H1dd3n_Pr06r4m!!!}i,
LKSCS{H1dd3n_Pr06r4m!!!}.py
LKSCS{H1dd3n_P
C:\Users\ADMIN~1\AppData\Local\Temp\_MEI25242\LKSCS{H1dd3n_Pr06r4m!!!}.py
"C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe"
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.pkg
LKSCS{H1dd3n_P
opiy-windows-manifest-filename LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
<assemblyIdentity type="win32" name="LKSCS{H1dd3n_Pr06r4m!!!}" processorArchitecture="x86" version="1.0.0.0"/>
LKSCS{H1dd3n_P
LKSCS{H1dd3n_P
LKSCS{H1dd3n_Pr06r4m!!!}i,
LKSCS{H1dd3n_Pr06r4m!!!}.py
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:/LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:/LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:/LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.pkg
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe?7306481
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
"C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe"
C:\LKSCS{H1dd3n_Pr06r4m!!!}.exe
opiy-windows-manifest-filename LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
sLKSCS{H1dd3n_Pr06r4m!!!}
bLKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
LKSCS{H1dd3n_Pr06r4m!!!}.exe
LKSCS{H1dd3n_Pr06r4m!!!}.exe.manifest
C:\Users\ADMIN~1\AppData\Local\Temp\_MEI25242\LKSCS{H1dd3n_Pr06r4m!!!}.py
C:/LKSCS{H1dd3n_Pr06r4m!!!}.exe
```

Cara kedua :

Menggunakan Volatility (<https://www.volatilityfoundation.org/>) untuk melakukan proses forensic hasil file dump memory komputer tersebut.

Pertama analisa OS yang digunakan dengan perintah sebagai berikut :

```
./vol.py -f memory.dmp imageinfo
```

```
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemory (Kernel AS)
      AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
      AS Layer3 : FileAddressSpace (/home/alchemist/Desktop/volatility/memory.dmp)
      PAE type : No PAE
      DTB : 0x185000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2021-06-03 17:52:26 UTC+0000
      Image local date and time : 2021-06-03 10:52:26 -0700
```

Sistem operasi yang digunakan adalah Windows 7 Service Pack 1 dengan arsitektur x86.

Selanjutnya, melihat proses yang running dari komputer tersebut menggunakan perintah sebagai berikut :

```
./vol.py -f memory.dmp --profile=Win7SP1x86 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x83f2f4a0	System	4	0	113	474		0	2021-06-03 17:51:32 UTC+0000	
0x8508c020	smss.exe	316	4	2	34		0	2021-06-03 17:51:32 UTC+0000	
0x867eb030	csrss.exe	400	392	12	362	0	0	2021-06-03 17:51:34 UTC+0000	
0x90024030	csrss.exe	452	444	12	231	1	0	2021-06-03 17:51:35 UTC+0000	
0x90030030	wininit.exe	460	392	4	88	0	0	2021-06-03 17:51:35 UTC+0000	
0x9004bd20	winlogon.exe	508	444	5	123	1	0	2021-06-03 17:51:35 UTC+0000	
0x90095030	services.exe	556	460	7	191	0	0	2021-06-03 17:51:35 UTC+0000	
0x9009a770	lsass.exe	564	460	10	481	0	0	2021-06-03 17:51:36 UTC+0000	
0x900ac1a0	lsm.exe	580	460	10	152	0	0	2021-06-03 17:51:36 UTC+0000	
0x901a2030	svchost.exe	680	556	13	369	0	0	2021-06-03 17:51:46 UTC+0000	
0x901ac030	VBoxService.exe	744	556	12	152	0	0	2021-06-03 17:51:47 UTC+0000	
0x901be770	svchost.exe	812	556	7	247	0	0	2021-06-03 17:51:47 UTC+0000	
0x901ebc70	svchost.exe	912	556	21	397	0	0	2021-06-03 17:51:47 UTC+0000	
0x90307030	svchost.exe	948	556	24	495	0	0	2021-06-03 17:51:47 UTC+0000	
0x90313030	svchost.exe	976	556	15	321	0	0	2021-06-03 17:51:47 UTC+0000	
0x90311330	svchost.exe	1016	556	29	706	0	0	2021-06-03 17:51:47 UTC+0000	
0x9032dd20	audiodg.exe	1092	912	5	131	0	0	2021-06-03 17:51:47 UTC+0000	
0x90347940	svchost.exe	1148	556	6	120	0	0	2021-06-03 17:51:47 UTC+0000	
0x9036c2b8	svchost.exe	1280	556	17	361	0	0	2021-06-03 17:51:47 UTC+0000	
0x903c89e0	spoolsv.exe	1432	556	15	309	0	0	2021-06-03 17:51:47 UTC+0000	
0x903dalf8	svchost.exe	1460	556	20	323	0	0	2021-06-03 17:51:47 UTC+0000	
0x9c036030	svchost.exe	1576	556	9	221	0	0	2021-06-03 17:51:48 UTC+0000	
0x9c08fd20	taskhost.exe	1744	556	10	174	1	0	2021-06-03 17:51:48 UTC+0000	
0x9c0c0030	dwm.exe	1888	948	5	100	1	0	2021-06-03 17:51:48 UTC+0000	
0x9c0b7d20	explorer.exe	1964	1872	34	849	1	0	2021-06-03 17:51:48 UTC+0000	
0x9c185030	VBoxTray.exe	708	1964	15	156	1	0	2021-06-03 17:51:50 UTC+0000	
0x84f36d20	SearchIndexer.	2324	556	13	611	0	0	2021-06-03 17:51:56 UTC+0000	
0x9c253d20	SearchProtocol	2408	2324	7	278	0	0	2021-06-03 17:51:56 UTC+0000	
0x9c25ed20	SearchFilterHo	2428	2324	6	88	0	0	2021-06-03 17:51:56 UTC+0000	
0x9c27e1e8	LKSCS{H1dd3n_P	2524	1964	4	38	1	0	2021-06-03 17:51:57 UTC+0000	
0x9c15bcf8	conhost.exe	2536	452	2	53	1	0	2021-06-03 17:51:58 UTC+0000	
0x9c279d20	LKSCS{H1dd3n_P	2560	2524	5	101	1	0	2021-06-03 17:51:59 UTC+0000	
0x9c0b4d20	livekd.exe	3108	1964	5	65	1	0	2021-06-03 17:52:21 UTC+0000	
0x9c32e4f8	conhost.exe	3116	452	2	53	1	0	2021-06-03 17:52:21 UTC+0000	
0x9c303030	kd.exe	3144	3108	2	28	1	0	2021-06-03 17:52:25 UTC+0000	

Terdapat proses bernama LKSCS{H1dd3n_P yang dicurigai sebagai flag namun hanya sebagian. Untuk itu menggunakan perintah sebagai berikut ini untuk melihat file apa

saja yang ada didalam komputer tersebut, menggunakan command grep untuk outputnya hanya string yang diinginkan

```
./vol.py -f memory.dmp --profile=Win7SP1x86 filescan | grep LKSCS
```

```
Volatility Foundation Volatility Framework 2.6.1
0x00000000ec6a8e0      8      0 R--r-d \Device\HarddiskVolume2\LKSCS{H1dd3n_Pr06r4m!!!}.exe
0x00000000ef858e0      8      0 R--r-d \Device\HarddiskVolume2\LKSCS{H1dd3n_Pr06r4m!!!}.exe
```

FLAG : LKSCS{H1dd3n_Pr06r4m!!!}

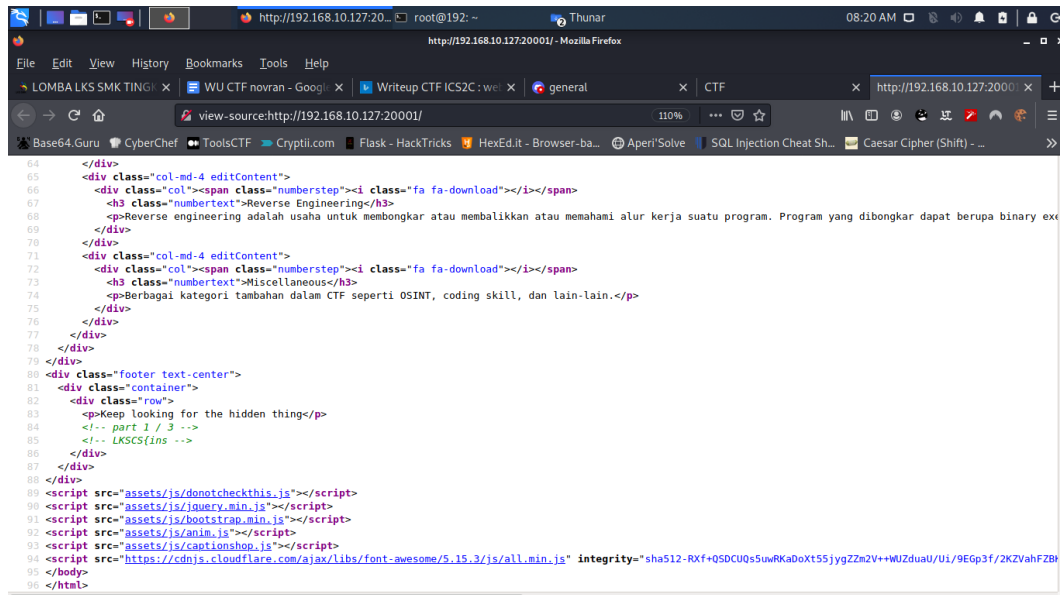
Web Exploitation

Know Your HTML

Cara menyelesaikan:

Web-know yourHTML-Diberikan sebuah halaman web mengenai sekilas CTF

ketika di source vource terdapat `<!-- part 1 / 3 -->` `<!-- LKSCS{ins` → sebuah flag yang terpisah. Dilihat dari part nya kalau flagnya dibagi menjadi 3 bagian, bagian pertama sudah ditemukan



```
64 </div>
65 <div class="col-md-4 editContent">
66 <div class="col"><span class="numberstep"><i class="fa fa-download"></i></span>
67 <h3 class="numbertext">Reverse Engineering</h3>
68 <p>Reverse engineering adalah usaha untuk membongkar atau membalikkan atau memahami alur kerja suatu program. Program yang dibongkar dapat berupa binary ex
69 </div>
70 </div>
71 <div class="col-md-4 editContent">
72 <div class="col"><span class="numberstep"><i class="fa fa-download"></i></span>
73 <h3 class="numbertext">Miscellaneous</h3>
74 <p>Berbagai kategori tambahan dalam CTF seperti OSINT, coding skill, dan lain-lain.</p>
75 </div>
76 </div>
77 </div>
78 </div>
79 </div>
80 <div class="footer text-center">
81 <div class="container">
82 <div class="row">
83 <p>Keep looking for the hidden things</p>
84 <!-- part 1 / 3 -->
85 <!-- LKSCS{ins -->
86 </div>
87 </div>
88 </div>
89 <script src="assets/js/donotcheckthis.js"></script>
90 <script src="assets/js/jquery.min.js"></script>
91 <script src="assets/js/bootstrap.min.js"></script>
92 <script src="assets/js/anim.js"></script>
93 <script src="assets/js/cautionshop.js"></script>
94 <script src="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.3/js/all.min.js" integrity="sha512-Rx+00Q55UwRkaDoxit55jygg22m2V++WU2duaU/Ui/9EGp3f/2KZVahFZB
95 </body>
96 </html>
```

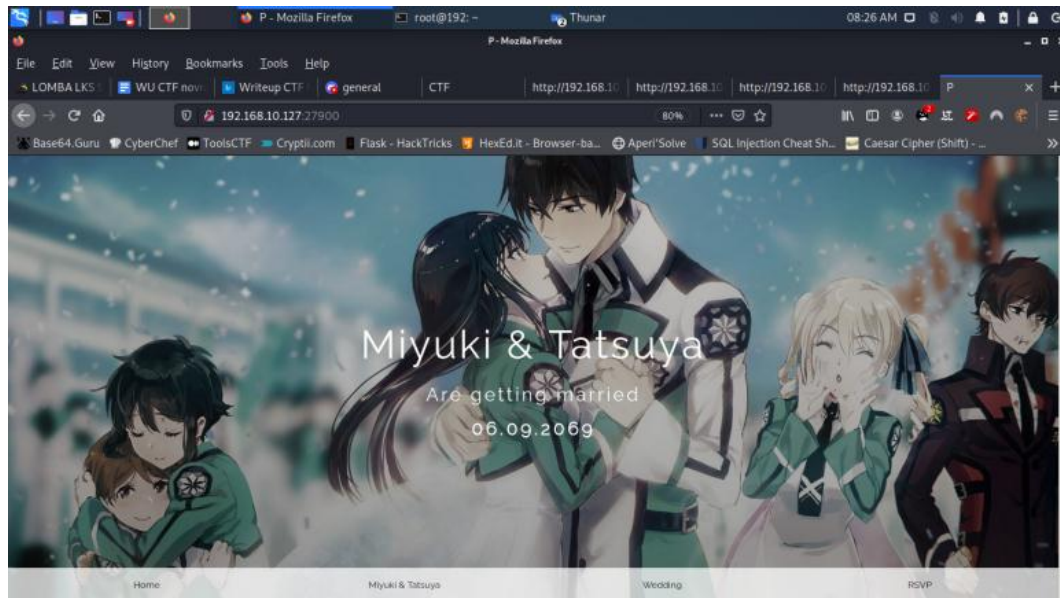
pada link href yang `"assets/css/donotseeme.css"` ketika kami buka terdapat flag yang ketiga yaitu `/* part 3 / 3 */ /* _dulu_pak_bos} */`

pada link yang `<script src="assets/js/donotcheckthis.js"></script>` ketika kami buka kami mendapatkan flag yang keduanya `// part 2 / 3 // pect_html`



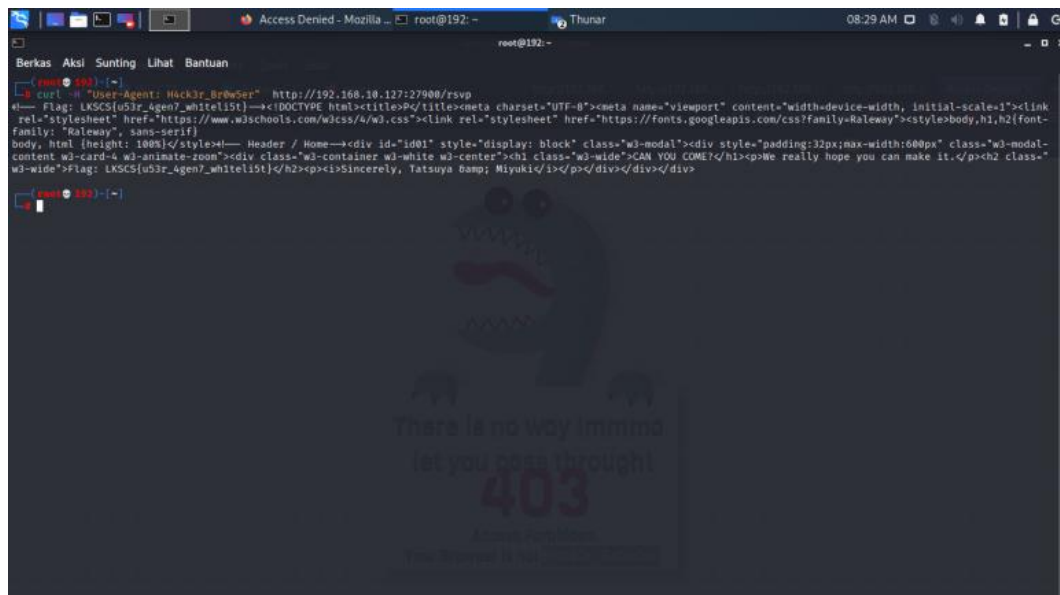
FLAG : `LKSCS{inspect_html_dulu_pak_bos}`

Invalid Browser



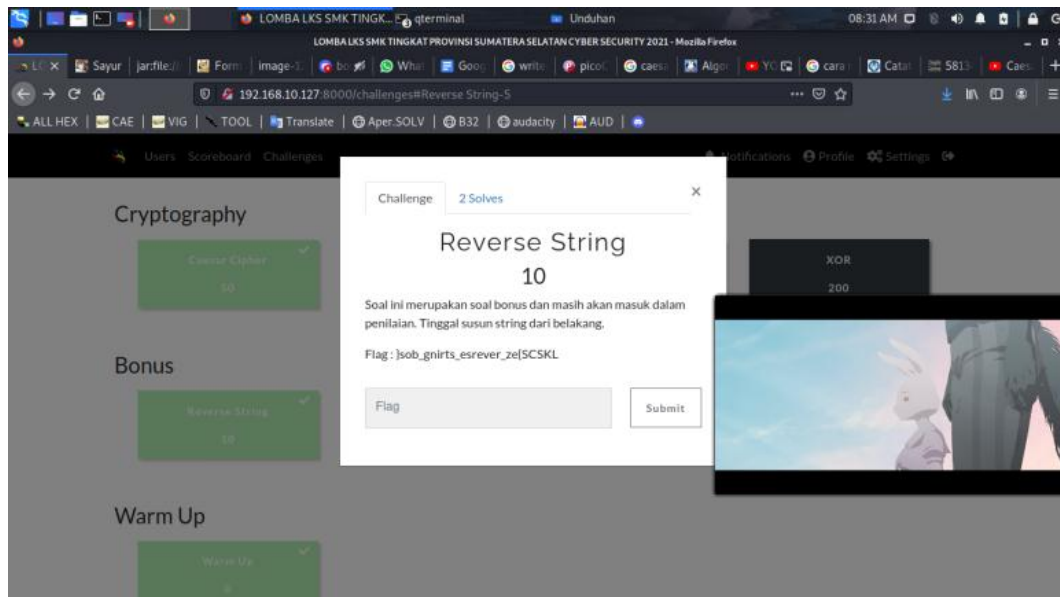
Cara menyelesaikan:

Pada soal ini kami mendapatkan invalid browser yang dimana kisi soal terdapat User-Agent maka melakukan bypass UA untuk mendapatkan flag



Flag : LKSCS{u53r_4gen7_wh1teli5t}

BONUS



Cara Menyelesaikan

Reverse String menyusun kata

Flag : LKSCS{ez_reverse_string_bos}