Malware-traffic-analysis-net Exercise

STEELCOFFEE

https://www.malware-traffic-analysis.net/2020/04/24/index.html

2540118486 -	Adam Aji Purnama
2301868983 -	Christian
2540119715 -	Kenn Christoval C
2540123302 -	I Pasek Made G.P.P
2501972524 -	Stephen Mario Wijaya

Scenario

LAN segment data:

LAN segment range: 10.0.0.0/24 (10.0.0.0 through 10.0.0.255)
Domain: steelcoffee.net
Domain controller: 10.0.0.10 — SteelCoffee-DC
LAN segment gateway: 10.0.0.1
LAN segment broadcast address: 10.0.0.255

Goals :

There are three clients in this month’s exercise pcap.

- Which two clients are Windows hosts, and what are the associated user account names?
- Which one of these two Windows clients was infected?
- What type of malware was that Windows client infected with?
- Is there any exposed credentials?

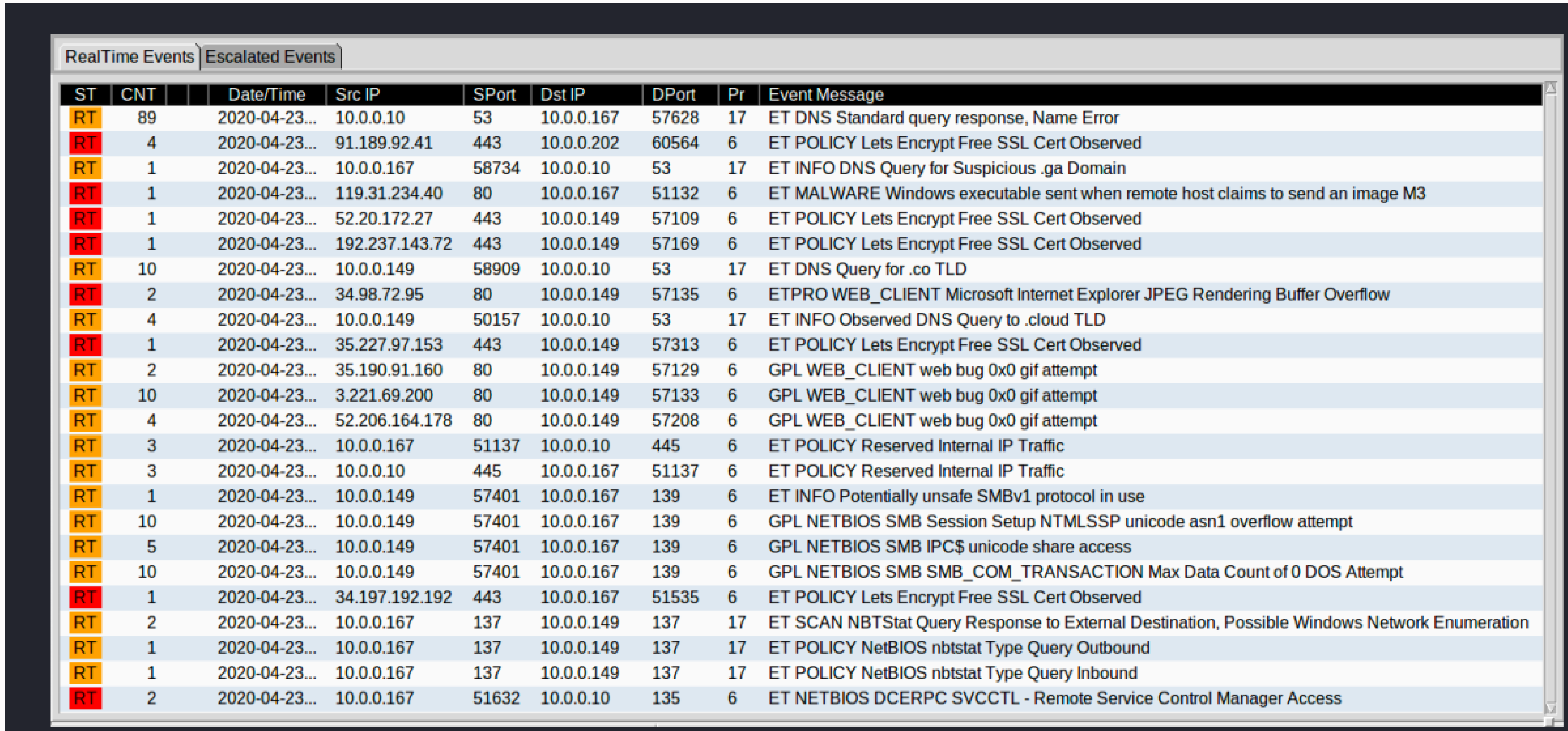
Tool

Wireshark

NetworkMiner

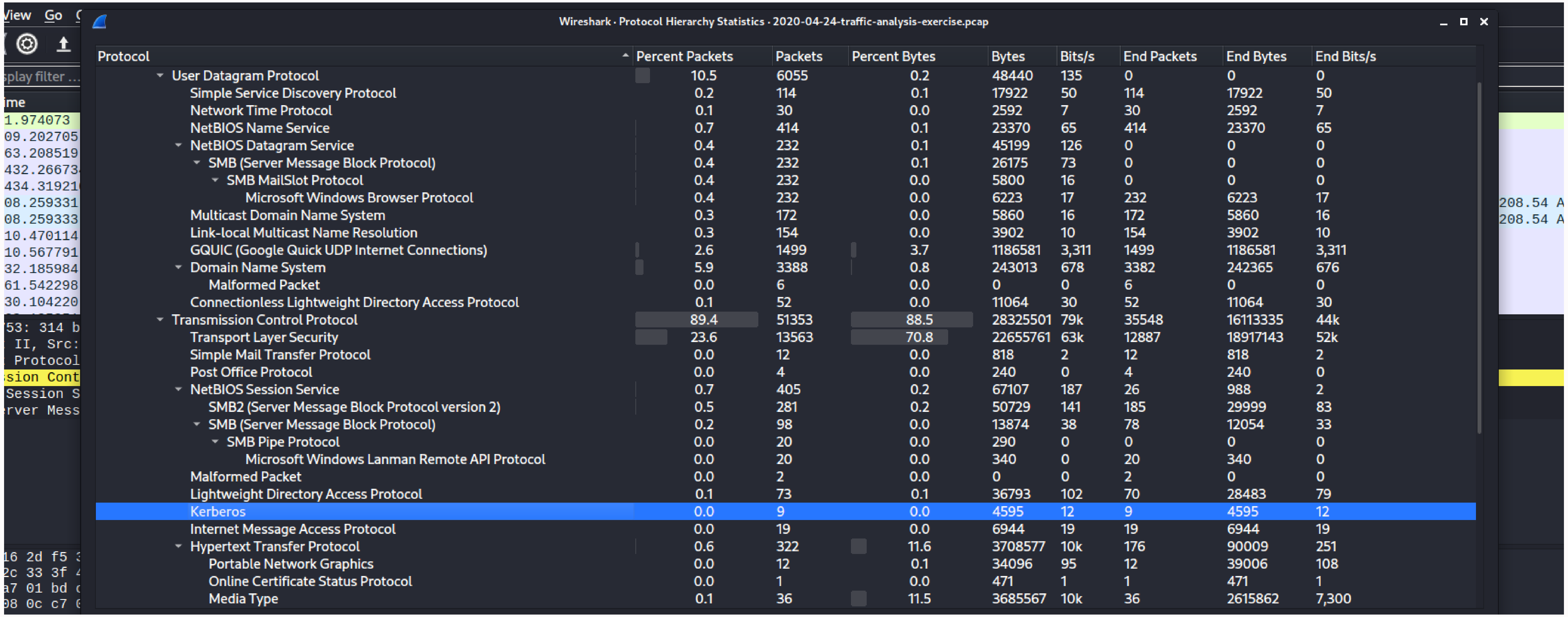
Analysis

Alert.jpg



ST	CNT			Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	89			2020-04-23...	10.0.0.10	53	10.0.0.167	57628	17	ET DNS Standard query response, Name Error
RT	4			2020-04-23...	91.189.92.41	443	10.0.0.202	60564	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	1			2020-04-23...	10.0.0.167	58734	10.0.0.10	53	17	ET INFO DNS Query for Suspicious .ga Domain
RT	1			2020-04-23...	119.31.234.40	80	10.0.0.167	51132	6	ET MALWARE Windows executable sent when remote host claims to send an image M3
RT	1			2020-04-23...	52.20.172.27	443	10.0.0.149	57109	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	1			2020-04-23...	192.237.143.72	443	10.0.0.149	57169	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	10			2020-04-23...	10.0.0.149	58909	10.0.0.10	53	17	ET DNS Query for .co TLD
RT	2			2020-04-23...	34.98.72.95	80	10.0.0.149	57135	6	ETPRO WEB_CLIENT Microsoft Internet Explorer JPEG Rendering Buffer Overflow
RT	4			2020-04-23...	10.0.0.149	50157	10.0.0.10	53	17	ET INFO Observed DNS Query to .cloud TLD
RT	1			2020-04-23...	35.227.97.153	443	10.0.0.149	57313	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	2			2020-04-23...	35.190.91.160	80	10.0.0.149	57129	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	10			2020-04-23...	3.221.69.200	80	10.0.0.149	57133	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	4			2020-04-23...	52.206.164.178	80	10.0.0.149	57208	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	3			2020-04-23...	10.0.0.167	51137	10.0.0.10	445	6	ET POLICY Reserved Internal IP Traffic
RT	3			2020-04-23...	10.0.0.10	445	10.0.0.167	51137	6	ET POLICY Reserved Internal IP Traffic
RT	1			2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10			2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5			2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10			2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	1			2020-04-23...	34.197.192.192	443	10.0.0.167	51535	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	2			2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET SCAN NBTStat Query Response to External Destination, Possible Windows Network Enumeration
RT	1			2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET POLICY NetBIOS nbtstat Type Query Outbound
RT	1			2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET POLICY NetBIOS nbtstat Type Query Inbound
RT	2			2020-04-23...	10.0.0.167	51632	10.0.0.10	135	6	ET NETBIOS DCERPC SVCCTL - Remote Service Control Manager Access

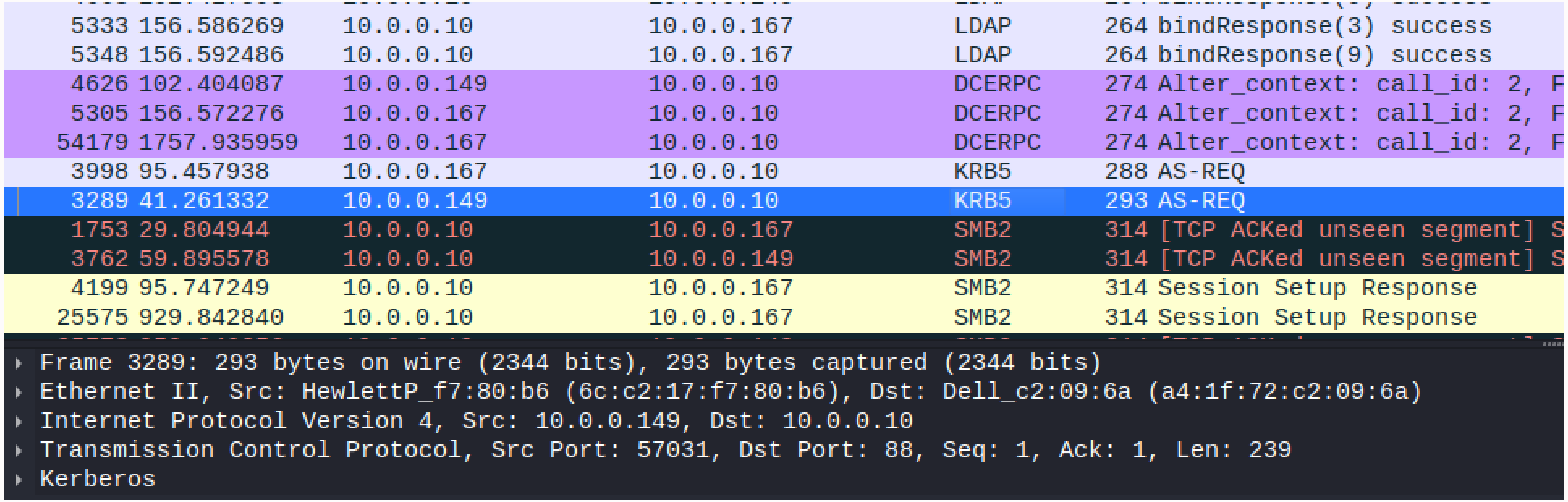
Pertama kita unzip file yang sudah di download, kemudian isi file tersebut terdapat file pcap dan juga alert.jpg . Dalam file alert.jpg berisi hasil alert dari IDS



Wireshark · Protocol Hierarchy Statistics · 2020-04-24-traffic-analysis-exercise.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
User Datagram Protocol	10.5	6055	0.2	48440	135	0	0	0
Simple Service Discovery Protocol	0.2	114	0.1	17922	50	114	17922	50
Network Time Protocol	0.1	30	0.0	2592	7	30	2592	7
NetBIOS Name Service	0.7	414	0.1	23370	65	414	23370	65
NetBIOS Datagram Service	0.4	232	0.1	45199	126	0	0	0
SMB (Server Message Block Protocol)	0.4	232	0.1	26175	73	0	0	0
SMB MailSlot Protocol	0.4	232	0.0	5800	16	0	0	0
Microsoft Windows Browser Protocol	0.4	232	0.0	6223	17	232	6223	17
Multicast Domain Name System	0.3	172	0.0	5860	16	172	5860	16
Link-local Multicast Name Resolution	0.3	154	0.0	3902	10	154	3902	10
GQUIC (Google Quick UDP Internet Connections)	2.6	1499	3.7	1186581	3,311	1499	1186581	3,311
Domain Name System	5.9	3388	0.8	243013	678	3382	242365	676
Malformed Packet	0.0	6	0.0	0	0	6	0	0
Connectionless Lightweight Directory Access Protocol	0.1	52	0.0	11064	30	52	11064	30
Transmission Control Protocol	89.4	51353	88.5	28325501	79k	35548	16113335	44k
Transport Layer Security	23.6	13563	70.8	22655761	63k	12887	18917143	52k
Simple Mail Transfer Protocol	0.0	12	0.0	818	2	12	818	2
Post Office Protocol	0.0	4	0.0	240	0	4	240	0
NetBIOS Session Service	0.7	405	0.2	67107	187	26	988	2
SMB2 (Server Message Block Protocol version 2)	0.5	281	0.2	50729	141	185	29999	83
SMB (Server Message Block Protocol)	0.2	98	0.0	13874	38	78	12054	33
SMB Pipe Protocol	0.0	20	0.0	290	0	0	0	0
Microsoft Windows Lanman Remote API Protocol	0.0	20	0.0	340	0	20	340	0
Malformed Packet	0.0	2	0.0	0	0	2	0	0
Lightweight Directory Access Protocol	0.1	73	0.1	36793	102	70	28483	79
Kerberos	0.0	9	0.0	4595	12	9	4595	12
Internet Message Access Protocol	0.0	19	0.0	6944	19	19	6944	19
Hypertext Transfer Protocol	0.6	322	11.6	3708577	10k	176	90009	251
Portable Network Graphics	0.0	12	0.1	34096	95	12	39006	108
Online Certificate Status Protocol	0.0	1	0.0	471	1	1	471	1
Media Type	0.1	36	11.5	3685567	10k	36	2615862	7,300

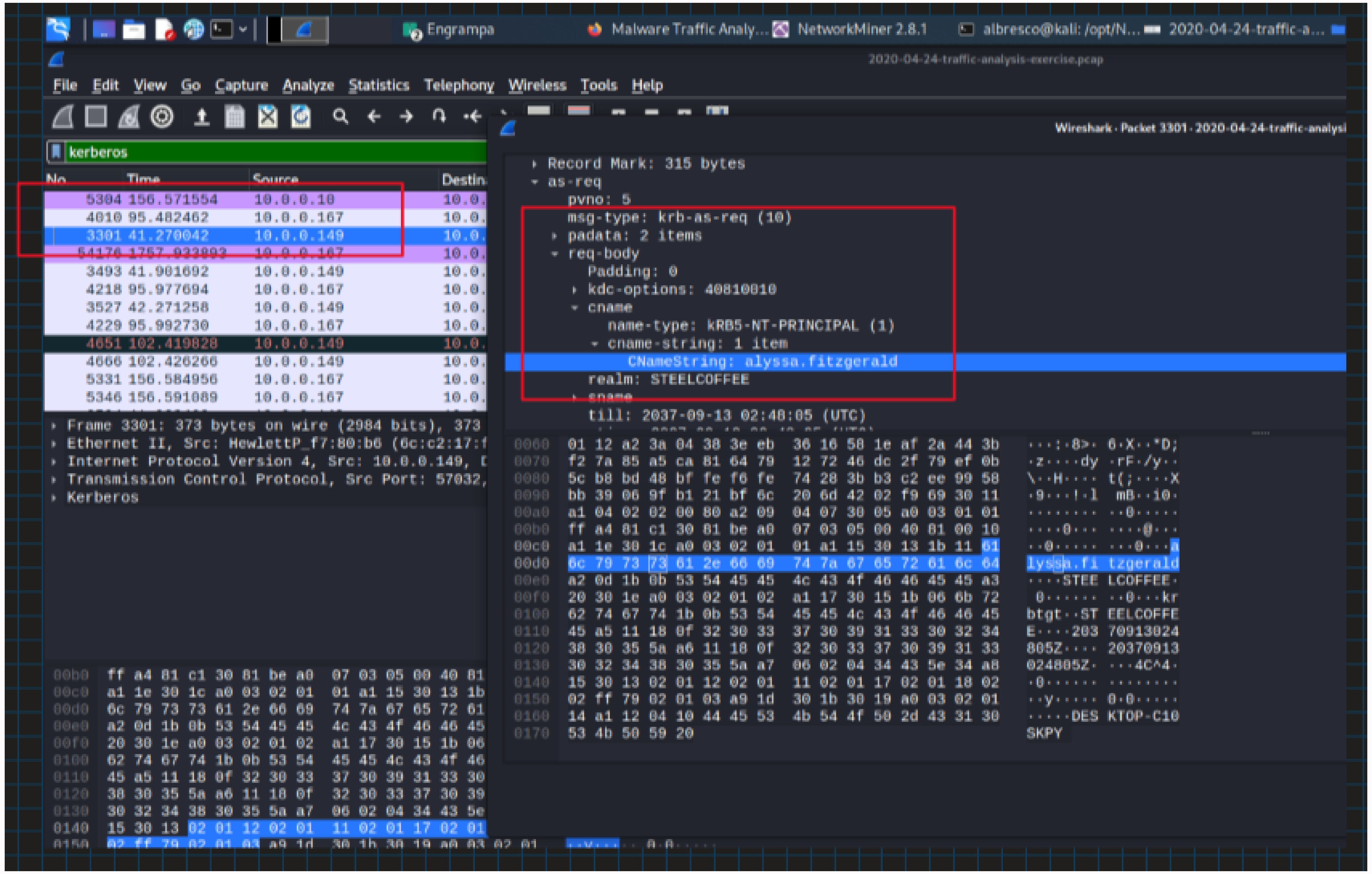
Karena kita ingin mencari windows host, maka kita dapat memerhatikan protokol hierarchy dari kerberos yang dimana dapat menyimpan nama akun yang sedang logged in ke dalam windows host di dalam network



```
 5333 156.586269   10.0.0.10     10.0.0.167    LDAP     264 bindResponse(3) success
 5348 156.592486   10.0.0.10     10.0.0.167    LDAP     264 bindResponse(9) success
 4626 102.404087   10.0.0.149    10.0.0.10     DCERPC   274 Alter_context: call_id: 2, F
 5305 156.572276   10.0.0.167    10.0.0.10     DCERPC   274 Alter_context: call_id: 2, F
54179 1757.935959  10.0.0.167    10.0.0.10     DCERPC   274 Alter_context: call_id: 2, F
 3998 95.457938    10.0.0.167    10.0.0.10     KRB5     288 AS-REQ
 3289 41.261332    10.0.0.149    10.0.0.10     KRB5     293 AS-REQ
 1753 29.804944    10.0.0.10     10.0.0.167    SMB2     314 [TCP ACKed unseen segment] S
 3762 59.895578    10.0.0.10     10.0.0.149    SMB2     314 [TCP ACKed unseen segment] S
 4199 95.747249    10.0.0.10     10.0.0.167    SMB2     314 Session Setup Response
25575 929.842840   10.0.0.10     10.0.0.167    SMB2     314 Session Setup Response
```

```
▸ Frame 3289: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits)
▸ Ethernet II, Src: HewlettP_f7:80:b6 (6c:c2:17:f7:80:b6), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
▸ Internet Protocol Version 4, Src: 10.0.0.149, Dst: 10.0.0.10
▸ Transmission Control Protocol, Src Port: 57031, Dst Port: 88, Seq: 1, Ack: 1, Len: 239
▸ Kerberos
```

Disini kita dapat melihat kerberos paket adalah AS-REQ (Authentication Service Request) yang dikirim ke KDC (Key Distribution Center) dari IP 10.0.0.149


Engrampa
Malware Traffic Analy...
NetworkMiner 2.8.1
albresco@kali: /opt/N...
2020-04-24-traffic-a...
2020-04-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 3301 · 2020-04-24-traffic-analysi

```
kerberos
```

```
No.    Time          Source       Destin
 5304 156.571554   10.0.0.10    10.0.
 4010 95.482462    10.0.0.167   10.0.
 3301 41.270042    10.0.0.149   10.0.
54176 1757.933893  10.0.0.167   10.0.
 3493 41.901692    10.0.0.149   10.0.
 4218 95.977694    10.0.0.167   10.0.
 3527 42.271258    10.0.0.149   10.0.
 4229 95.992730    10.0.0.167   10.0.
 4651 102.419828   10.0.0.149   10.0.
 4666 102.426266   10.0.0.149   10.0.
 5331 156.584956   10.0.0.167   10.0.
 5346 156.591089   10.0.0.167   10.0.
```

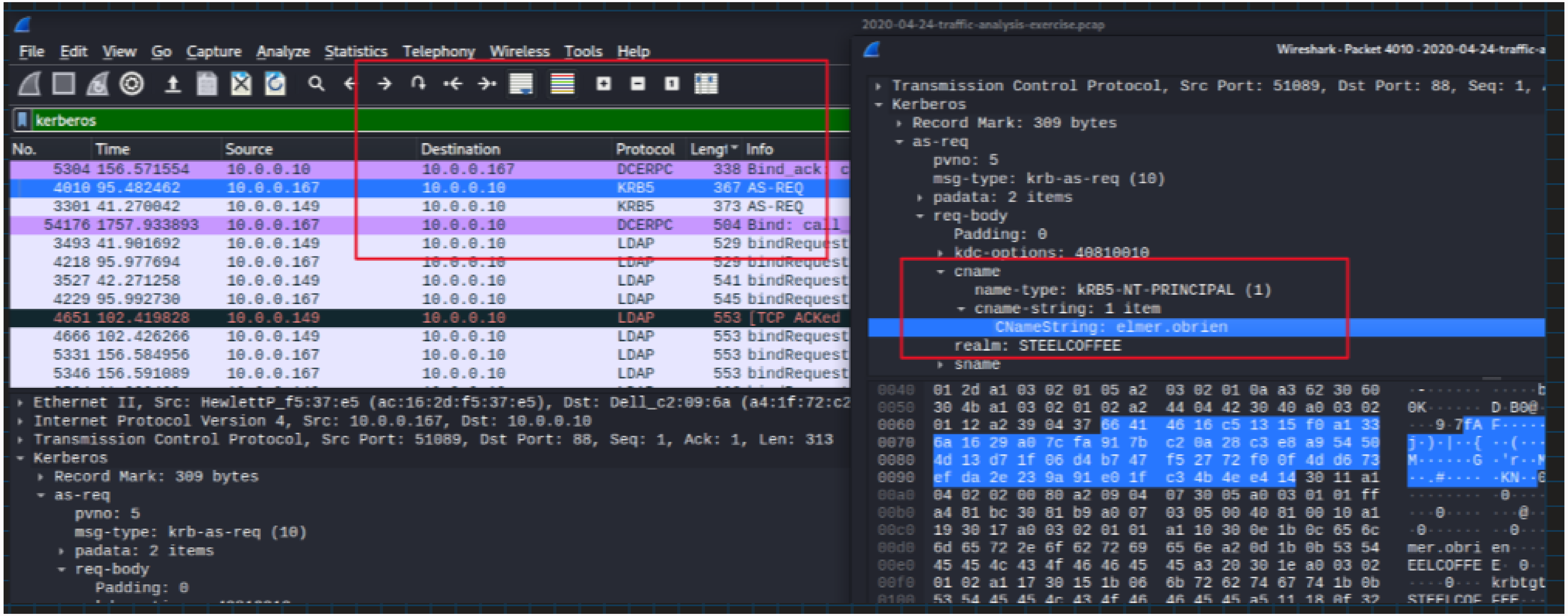
```
› Frame 3301: 373 bytes on wire (2984 bits), 373
› Ethernet II, Src: HewlettP_f7:80:b6 (6c:c2:17:f
› Internet Protocol Version 4, Src: 10.0.0.149, D
› Transmission Control Protocol, Src Port: 57032,
› Kerberos
```

```
00b0  ff a4 81 c1 30 81 be a0  07 03 05 00 40 81
00c0  a1 1e 30 1c a0 03 02 01  01 a1 15 30 13 1b
00d0  6c 79 73 73 61 2e 66 69  74 7a 67 65 72 61
00e0  a2 0d 1b 0b 53 54 45 45  4c 43 4f 46 46 45
00f0  20 30 1e a0 03 02 01 02  a1 17 30 15 1b 06
0100  62 74 67 74 1b 0b 53 54  45 45 4c 43 4f 46
0110  45 a5 11 18 0f 32 30 33  37 30 39 31 33 30
0120  38 30 35 5a a6 11 18 0f  32 30 33 37 30 39
0130  30 32 34 38 30 35 5a a7  06 02 04 34 43 5e
0140  15 30 13 02 01 12 02 01  11 02 01 17 02 01
0150  02 ff 79 02 01 03 a9 1d  30 1b 30 19 a0 03 02 01
```

```
› Record Mark: 315 bytes
⌄ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  › padata: 2 items
  ⌄ req-body
      Padding: 0
    › kdc-options: 40810010
    ⌄ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ⌄ cname-string: 1 item
          CNameString: alyssa.fitzgerald
      realm: STEELCOFFEE
    › sname
      till: 2037-09-13 02:48:05 (UTC)
```

```
0060  01 12 a2 3a 04 38 3e eb  36 16 58 1e af 2a 44 3b   ···:·8>· 6·X··*D;
0070  f2 7a 85 a5 ca 81 64 79  12 72 46 dc 2f 79 ef 0b   ·z····dy ·rF·/y··
0080  5c b8 bd 48 bf fe f6 fe  74 28 3b b3 c2 ee 99 58   \··H···· t(;····X
0090  bb 39 06 9f b1 21 bf 6c  20 6d 42 02 f9 69 30 11   ·9···!·l  mB··i0·
00a0  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
00b0  ff a4 81 c1 30 81 be a0  07 03 05 00 40 81 00 10   ····0··· ····@···
00c0  a1 1e 30 1c a0 03 02 01  01 a1 15 30 13 1b 11 61   ··0····· ···0···a
00d0  6c 79 73 73 61 2e 66 69  74 7a 67 65 72 61 6c 64   lyssa.fi tzgerald
00e0  a2 0d 1b 0b 53 54 45 45  4c 43 4f 46 46 45 45 a3   ····STEE LCOFFEE·
00f0  20 30 1e a0 03 02 01 02  a1 17 30 15 1b 06 6b 72    0······ ··0···kr
0100  62 74 67 74 1b 0b 53 54  45 45 4c 43 4f 46 46 45   btgt··ST EELCOFFE
0110  45 a5 11 18 0f 32 30 33  37 30 39 31 33 30 32 34   E····203 70913024
0120  38 30 35 5a a6 11 18 0f  32 30 33 37 30 39 31 33   805Z···· 20370913
0130  30 32 34 38 30 35 5a a7  06 02 04 34 43 5e 34 a8   024805Z· ···4C^4·
0140  15 30 13 02 01 12 02 01  11 02 01 17 02 01 18 02   ·0······ ········
0150  02 ff 79 02 01 03 a9 1d  30 1b 30 19 a0 03 02 01   ··y····· 0·0·····
0160  14 a1 12 04 10 44 45 53  4b 54 4f 50 2d 43 31 30   ·····DES KTOP-C10
0170  53 4b 50 59 20                                      SKPY
```

Disini dapat kita lihat pada ip 10.0.0.149 terdapat sebuah kerberos packet dengan info AS-REQ. Yang dimana pada field CNAMESTRING terdapat sebuah username dengan nama “alyssa.fitzgerald”


2020-04-24-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 4010 · 2020-04-24-traffic-a

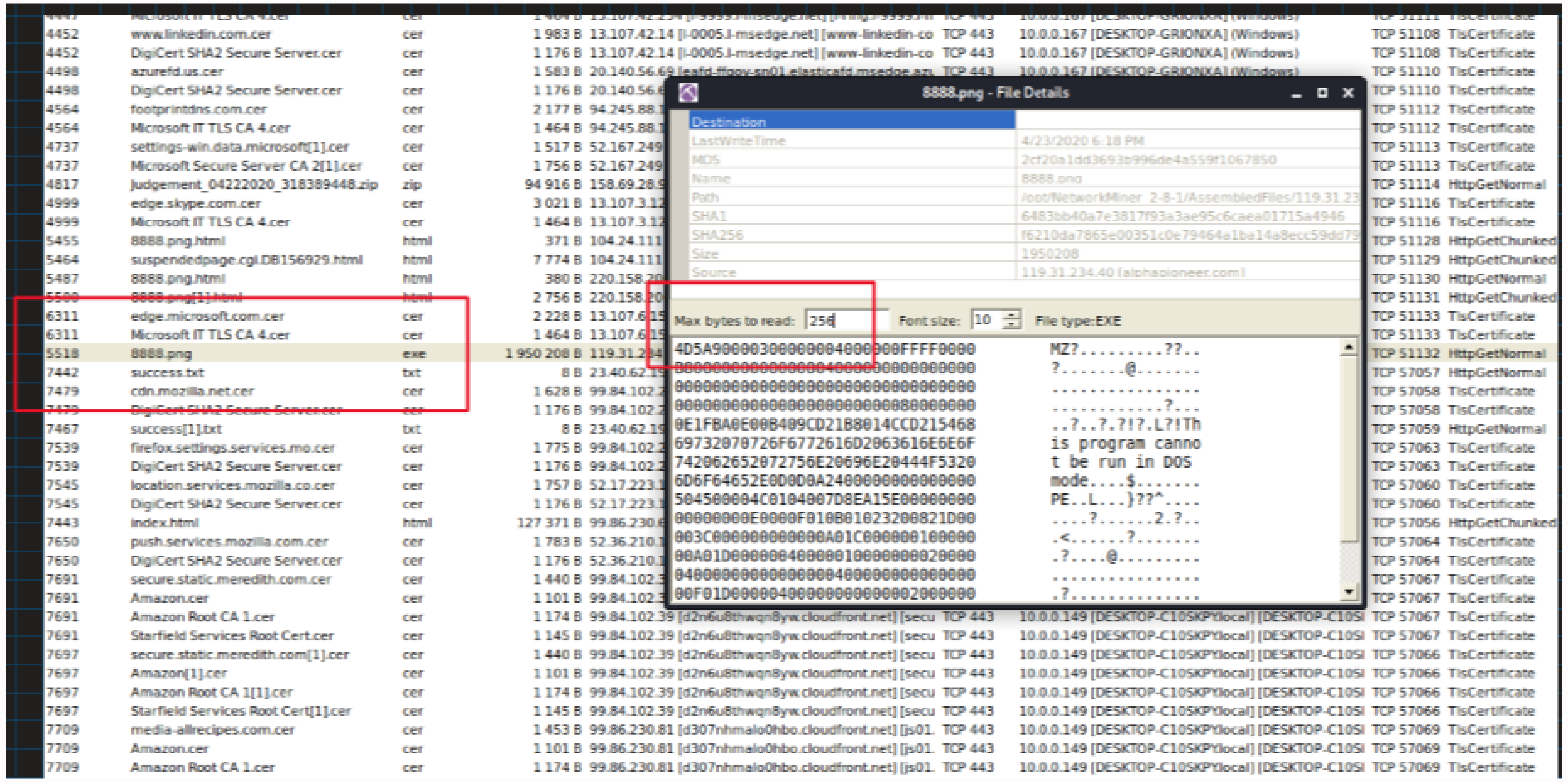
```
kerberos

No.    Time          Source        Destination   Protocol  Lengt  Info
 5304  156.571554    10.0.0.10     10.0.0.167    DCERPC    338 Bind_ack: c
 4010  95.482462     10.0.0.167    10.0.0.10     KRB5      367 AS-REQ
 3301  41.270042     10.0.0.149    10.0.0.10     KRB5      373 AS-REQ
54176  1757.933893   10.0.0.167    10.0.0.10     DCERPC    504 Bind: call_
 3493  41.901692     10.0.0.149    10.0.0.10     LDAP      529 bindRequest
 4218  95.977694     10.0.0.167    10.0.0.10     LDAP      529 bindRequest
 3527  42.271258     10.0.0.149    10.0.0.10     LDAP      541 bindRequest
 4229  95.992730     10.0.0.167    10.0.0.10     LDAP      545 bindRequest
 4651  102.419828    10.0.0.149    10.0.0.10     LDAP      553 [TCP ACKed
 4666  102.426266    10.0.0.149    10.0.0.10     LDAP      553 bindRequest
 5331  156.584956    10.0.0.167    10.0.0.10     LDAP      553 bindRequest
 5346  156.591089    10.0.0.167    10.0.0.10     LDAP      553 bindRequest
```

```
▸ Ethernet II, Src: HewlettP_f5:37:e5 (ac:16:2d:f5:37:e5), Dst: Dell_c2:09:6a (a4:1f:72:c2
▸ Internet Protocol Version 4, Src: 10.0.0.167, Dst: 10.0.0.10
▸ Transmission Control Protocol, Src Port: 51089, Dst Port: 88, Seq: 1, Ack: 1, Len: 313
▾ Kerberos
  ▸ Record Mark: 309 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 2 items
    ▾ req-body
        Padding: 0
```

```
▸ Transmission Control Protocol, Src Port: 51089, Dst Port: 88, Seq: 1,
▾ Kerberos
  ▸ Record Mark: 309 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 2 items
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: elmer.obrien
        realm: STEELCOFFEE
      ▸ sname
```

```
0040  01 2d a1 03 02 01 05 a2  03 02 01 0a a3 62 30 60   ·-······ ·····b
0050  30 4b a1 03 02 01 02 a2  44 04 42 30 40 a0 03 02   0K······ D·B0@·
0060  01 12 a2 39 04 37 66 41  46 16 c5 13 15 f0 a1 33   ···9·7fA F·····
0070  6a 16 29 a0 7c fa 91 7b  c2 0a 28 c3 e8 a9 54 50   j·)·|··{ ··(····
0080  4d 13 d7 1f 06 d4 b7 47  f5 27 72 f0 0f 4d d6 73   M······G ·'r··M
0090  ef da 2e 23 9a 91 e0 1f  c3 4b 4e e4 14 30 11 a1   ···.#···· ·KN··0
00a0  04 02 02 00 80 a2 09 04  07 30 05 a0 03 01 01 ff   ········ ·0····
00b0  a4 81 bc 30 81 b9 a0 07  03 05 00 40 81 00 10 a1   ···0···· ···@··
00c0  19 30 17 a0 03 02 01 01  a1 10 30 0e 1b 0c 65 6c   ·0······ ··0···
00d0  6d 65 72 2e 6f 62 72 69  65 6e a2 0d 1b 0b 53 54   mer.obri en····
00e0  45 45 4c 43 4f 46 46 45  45 a3 20 30 1e a0 03 02   EELCOFFE E· 0··
00f0  01 02 a1 17 30 15 1b 06  6b 72 62 74 67 74 1b 0b   ····0··· krbtgt
0100  53 54 45 45 4c 43 4f 46  46 45 45 a5 11 18 0f 32   STEELCOF FEE···
```

Dalam CNameString, kita mendapatkan username kedua yaitu “elmer.obrien”. sehingga untuk pertanyaan pertama kita sudah dapatkan 2 username “alyssa.fitzgerald” dan juga “elmer.obrien”.



[illegible]	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.42.254 [l-9999.l-msedge.net] [l-ring.l-9999.m	TCP 443	10.0.0.167 [DESKTOP-GRIONXA] (Windows)	TCP 51111	TlsCertificate
4452	www.linkedin.com.cer	cer	1 983 B	13.107.42.14 [l-0005.l-msedge.net] [www-linkedin-co	TCP 443	10.0.0.167 [DESKTOP-GRIONXA] (Windows)	TCP 51108	TlsCertificate
4452	DigiCert SHA2 Secure Server.cer	cer	1 176 B	13.107.42.14 [l-0005.l-msedge.net] [www-linkedin-co	TCP 443	10.0.0.167 [DESKTOP-GRIONXA] (Windows)	TCP 51108	TlsCertificate
4498	azurefd.us.cer	cer	1 583 B	20.140.56.69 [eafd-ffgov-sn01.elasticafd.msedge.azu	TCP 443	10.0.0.167 [DESKTOP-GRIONXA] (Windows)	TCP 51110	TlsCertificate
4498	DigiCert SHA2 Secure Server.cer	cer	1 176 B	20.140.56.6			TCP 51110	TlsCertificate
4564	footprintdns.com.cer	cer	2 177 B	94.245.88.1			TCP 51112	TlsCertificate
4564	Microsoft IT TLS CA 4.cer	cer	1 464 B	94.245.88.1			TCP 51112	TlsCertificate
4737	settings-win.data.microsoft[1].cer	cer	1 517 B	52.167.249			TCP 51113	TlsCertificate
4737	Microsoft Secure Server CA 2[1].cer	cer	1 756 B	52.167.249			TCP 51113	TlsCertificate
4817	Judgement_04222020_318389448.zip	zip	94 916 B	158.69.28.9			TCP 51114	HttpGetNormal
4999	edge.skype.com.cer	cer	3 021 B	13.107.3.12			TCP 51116	TlsCertificate
4999	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.3.12			TCP 51116	TlsCertificate
5455	8888.png.html	html	371 B	104.24.111			TCP 51128	HttpGetChunked
5464	suspendedpage.cgi.DB156929.html	html	7 774 B	104.24.111			TCP 51129	HttpGetChunked
5487	8888.png.html	html	380 B	220.158.20			TCP 51130	HttpGetNormal
5500	8888.png[1].html	html	2 756 B	220.158.20			TCP 51131	HttpGetChunked
6311	edge.microsoft.com.cer	cer	2 228 B	13.107.6.15			TCP 51133	TlsCertificate
6311	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.6.15			TCP 51133	TlsCertificate
5518	8888.png	exe	1 950 208 B	119.31.234			TCP 51132	HttpGetNormal
7442	success.txt	txt	8 B	23.40.62.19			TCP 57057	HttpGetNormal
7479	cdn.mozilla.net.cer	cer	1 628 B	99.84.102.2			TCP 57058	TlsCertificate
7479	DigiCert SHA2 Secure Server.cer	cer	1 176 B	99.84.102.2			TCP 57058	TlsCertificate
7467	success[1].txt	txt	8 B	23.40.62.19			TCP 57059	HttpGetNormal
7539	firefox.settings.services.mo.cer	cer	1 775 B	99.84.102.2			TCP 57063	TlsCertificate
7539	DigiCert SHA2 Secure Server.cer	cer	1 176 B	99.84.102.2			TCP 57063	TlsCertificate
7545	location.services.mozilla.co.cer	cer	1 757 B	52.17.223.1			TCP 57060	TlsCertificate
7545	DigiCert SHA2 Secure Server.cer	cer	1 176 B	52.17.223.1			TCP 57060	TlsCertificate
7443	index.html	html	127 371 B	99.86.230.6			TCP 57056	HttpGetChunked
7650	push.services.mozilla.com.cer	cer	1 783 B	52.36.210.1			TCP 57064	TlsCertificate
7650	DigiCert SHA2 Secure Server.cer	cer	1 176 B	52.36.210.1			TCP 57064	TlsCertificate
7691	secure.static.meredith.com.cer	cer	1 440 B	99.84.102.3			TCP 57067	TlsCertificate
7691	Amazon.cer	cer	1 101 B	99.84.102.3			TCP 57067	TlsCertificate
7691	Amazon Root CA 1.cer	cer	1 174 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57067	TlsCertificate
7691	Starfield Services Root Cert.cer	cer	1 145 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57067	TlsCertificate
7697	secure.static.meredith.com[1].cer	cer	1 440 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57066	TlsCertificate
7697	Amazon[1].cer	cer	1 101 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57066	TlsCertificate
7697	Amazon Root CA 1[1].cer	cer	1 174 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57066	TlsCertificate
7697	Starfield Services Root Cert[1].cer	cer	1 145 B	99.84.102.39 [d2n6u8thwqn8yw.cloudfront.net] [secu	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57066	TlsCertificate
7709	media-allrecipes.com.cer	cer	1 453 B	99.86.230.81 [d307nhmalo0hbo.cloudfront.net] [js01.	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57069	TlsCertificate
7709	Amazon.cer	cer	1 101 B	99.86.230.81 [d307nhmalo0hbo.cloudfront.net] [js01.	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57069	TlsCertificate
7709	Amazon Root CA 1.cer	cer	1 174 B	99.86.230.81 [d307nhmalo0hbo.cloudfront.net] [js01.	TCP 443	10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SI	TCP 57069	TlsCertificate

8888.png - File Details

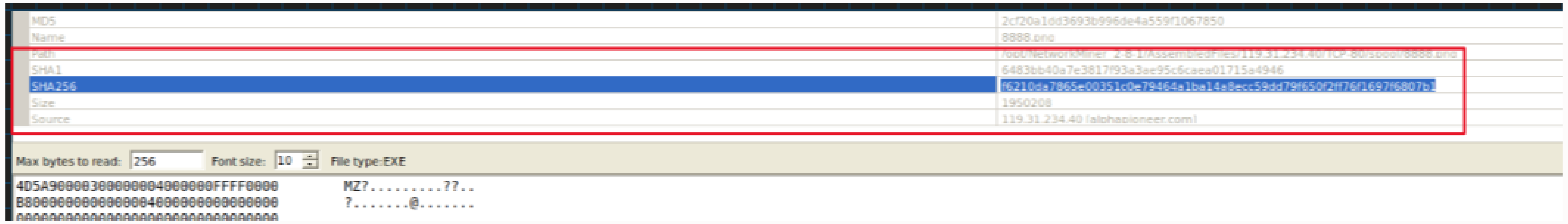
Destination	
LastWriteTime	4/23/2020 6:18 PM
MD5	2cf20a1dd3693b996de4a559f1067850
Name	8888.png
Path	/opt/NetworkMiner_2-8-1/AssembledFiles/119.31.23
SHA1	6483bb40a7e3817f93a3ae95c6caea01715a4946
SHA256	f6210da7865e00351c0e79464a1ba14a8ecc59dd79
Size	1950208
Source	119.31.234.40 [alphapioneer.com]

Max bytes to read: 256 Font size: 10 File type:EXE

```
4D5A90000300000004000000FFFF0000        MZ?.........??..
B8000000000000004000000000000000        ?.......@.......
00000000000000000000000000000000        ................
00000000000000000000000080000000        ............?...
0E1FBA0E00B409CD21B8014CCD215468        ..?..?.?!?.L?!Th
69732070726F6772616D2063616E6E6F        is program canno
742062652072756E20696E20444F5320        t be run in DOS 
6D6F64652E0D0D0A2400000000000000        mode....$.......
504500004C0104007D8EA15E00000000        PE..L...}??^....
00000000E0000F010B01023200821D00        ....?.......2.?..
003C000000000000A01C000000100000        .<......?.......
00A01D00000040000010000000020000        .?....@.........
04000000000000000400000000000000        ................
00F01D00000400000000000002000000        .?..............
```

Disini terdapat executable bernama "8888.png". Karena max byte to read defaultnya 1000 + bytes, maka kita adjust ke 256 bytes.

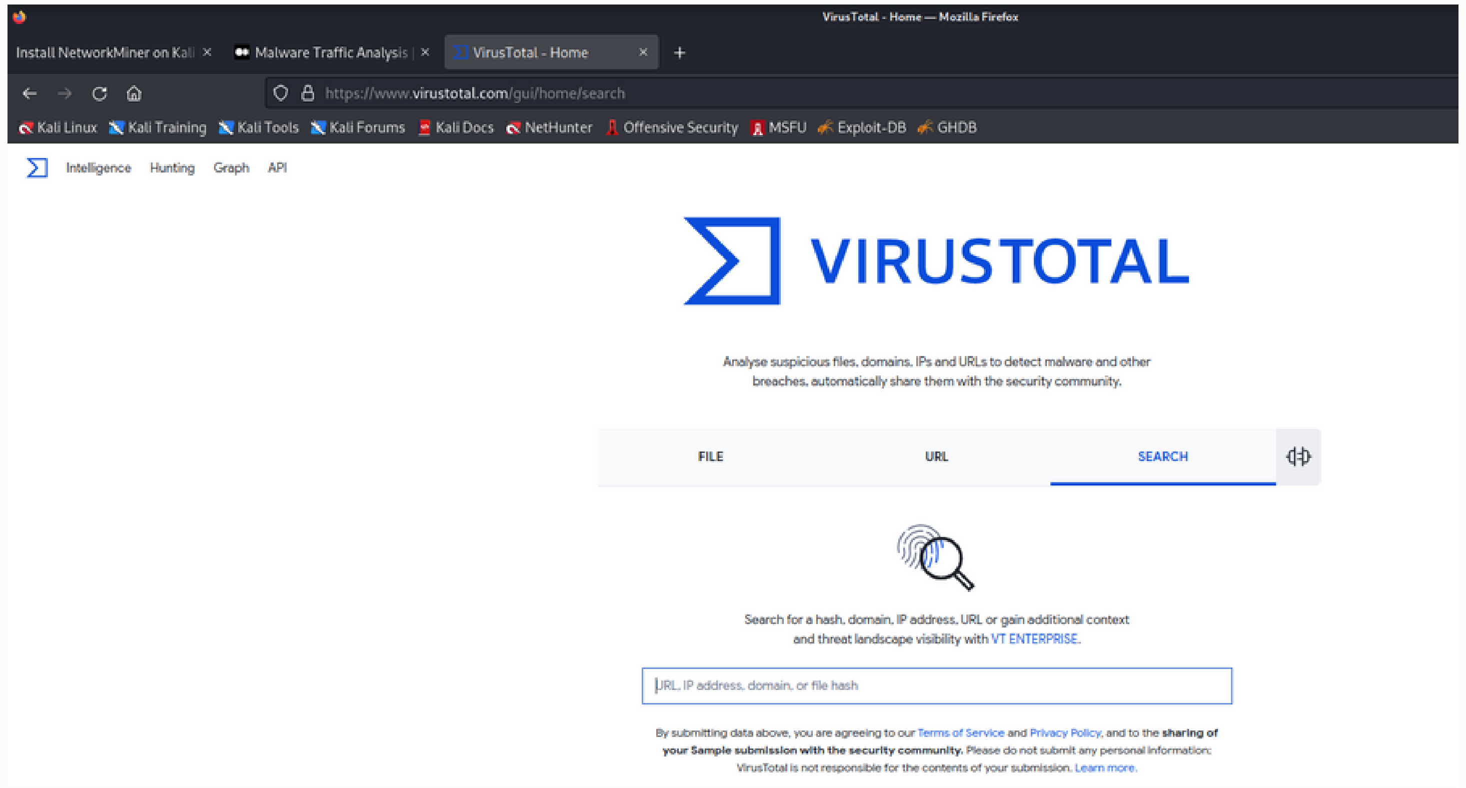
Lalu disini kita dapat mengambil SHA-256 hash dari executable tersebut



MD5	2cf20a1dd3693b996de4a559f1067850
Name	8888.png
Path	/opt/NetworkMiner_2-8-1/AssembledFiles/119.31.234.40/TCP-80/spool/8888.png
SHA1	6483bb40a7e3817f93a3ae95c6caea01715a4946
SHA256	f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
Size	1950208
Source	119.31.234.40 [alphapioneer.com]

Max bytes to read: 256 Font size: 10 File type:EXE

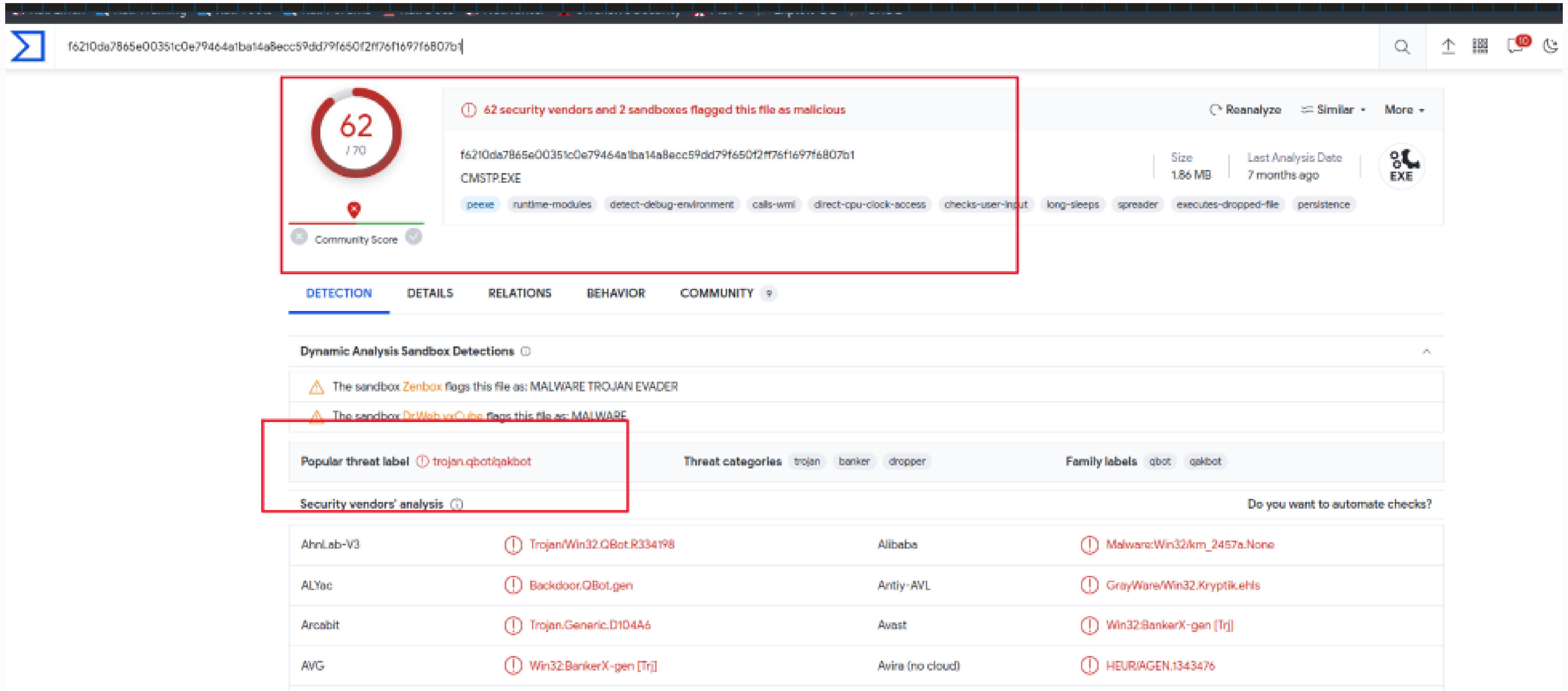
```
4D5A90000300000004000000FFFF0000        MZ?.........??..
B8000000000000004000000000000000        ?.......@.......
00000000000000000000000000000000
```



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with VT ENTERPRISE.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.



f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1

62 / 70

62 security vendors and 2 sandboxes flagged this file as malicious

f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
CMSTP.EXE

peexe runtime-modules detect-debug-environment calls-wmi direct-cpu-clock-access checks-user-input long-sleeps spreader executes-dropped-file persistence

Size 1.86 MB
Last Analysis Date 7 months ago

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE TROJAN EVADER

The sandbox DrWeb vxCube flags this file as: MALWARE

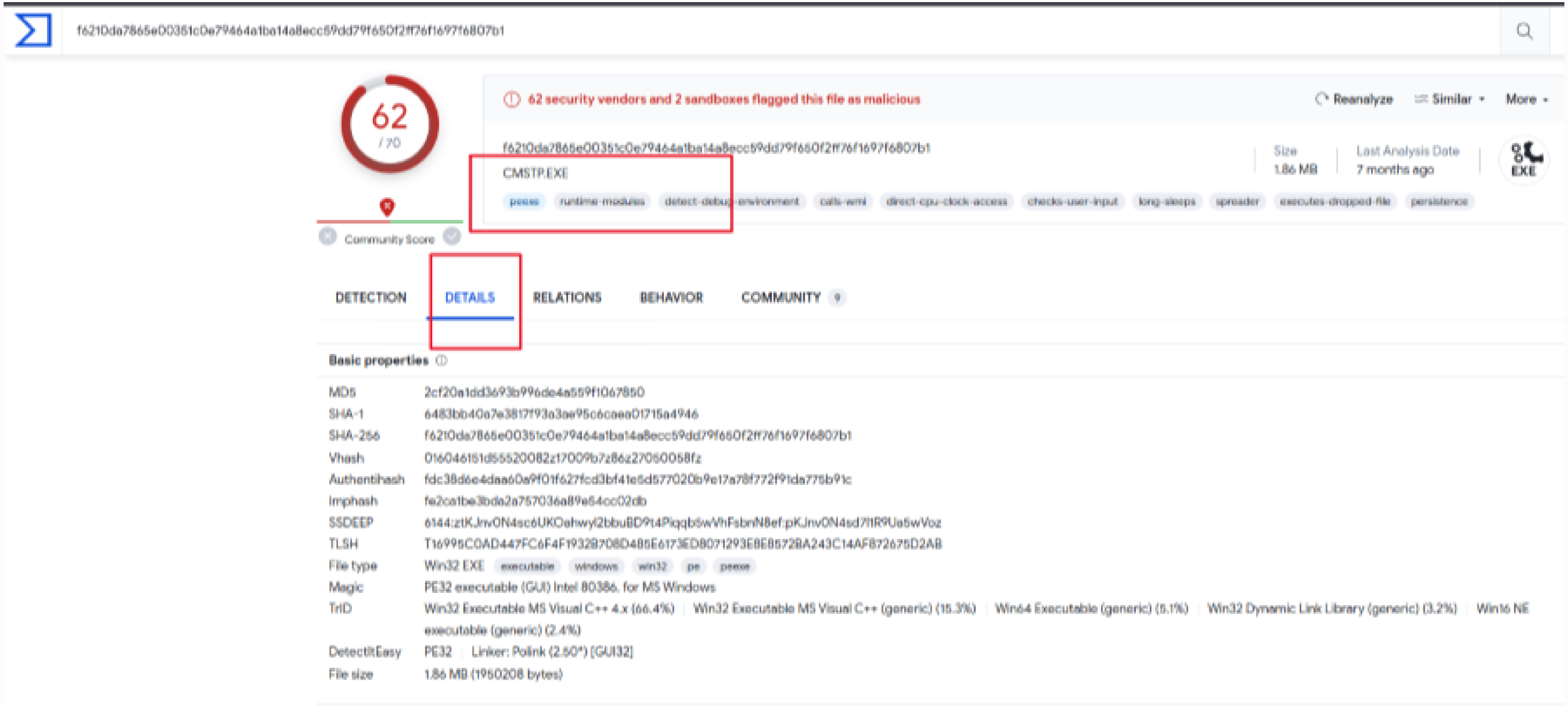
Popular threat label trojan.qbot/qakbot **Threat categories** trojan banker dropper **Family labels** qbot qakbot

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.QBot.R334198	Alibaba	Malware:Win32/km_2457a.None
ALYac	Backdoor.QBot.gen	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
Arcabit	Trojan.Generic.D104A6	Avast	Win32:BankerX-gen [Trj]
AVG	Win32:BankerX-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1343476

Setelah itu, kita akan cek di open source tools yang bernama Virus Total untuk melihat apakah file CMSTP.EXE malicious atau tidak. Hasil pengecekan menunjukkan bahwa tingkat maliciousnya sebesar 62/70 dan juga threat labelnya adalah trojan.qbot/qakbot.



62 security vendors and 2 sandboxes flagged this file as malicious

f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1

CMSTP.EXE

peexe runtime-modules detect-debug-environment calls-wmi direct-cpu-clock-access checks-user-input long-sleeps spreader executes-dropped-file persistence

Size 1.86 MB

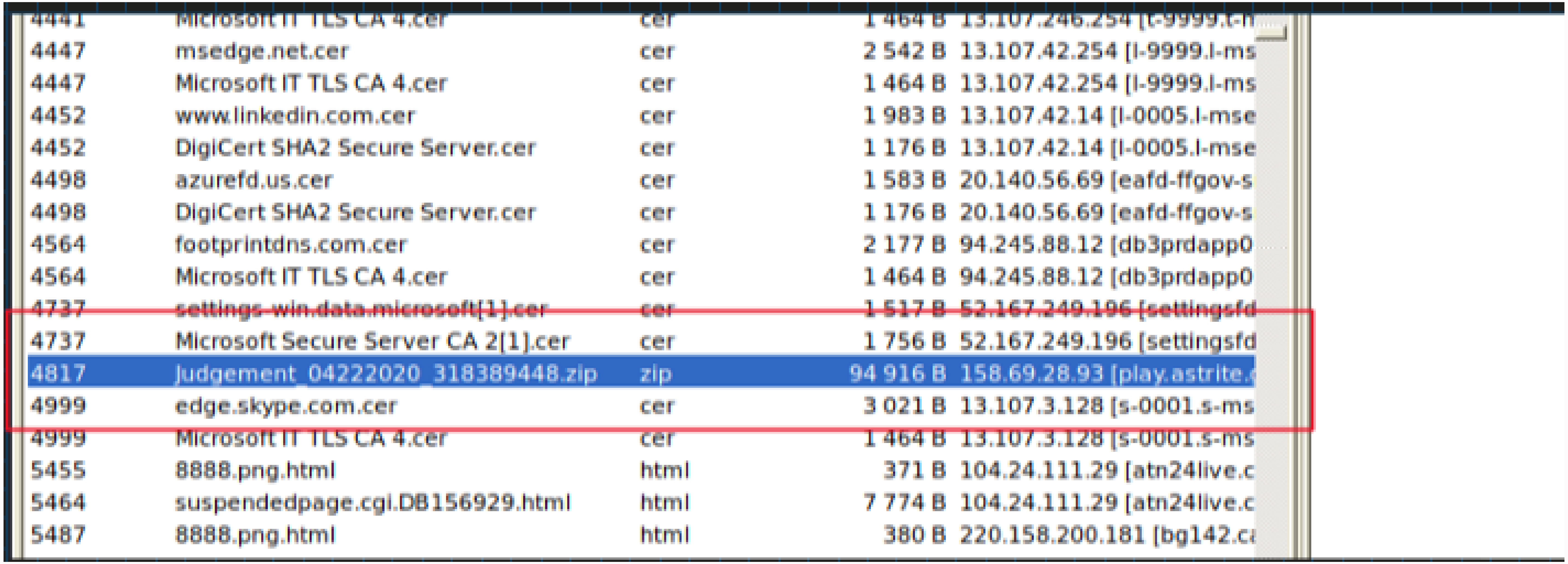
Last Analysis Date 7 months ago

EXE

Basic properties

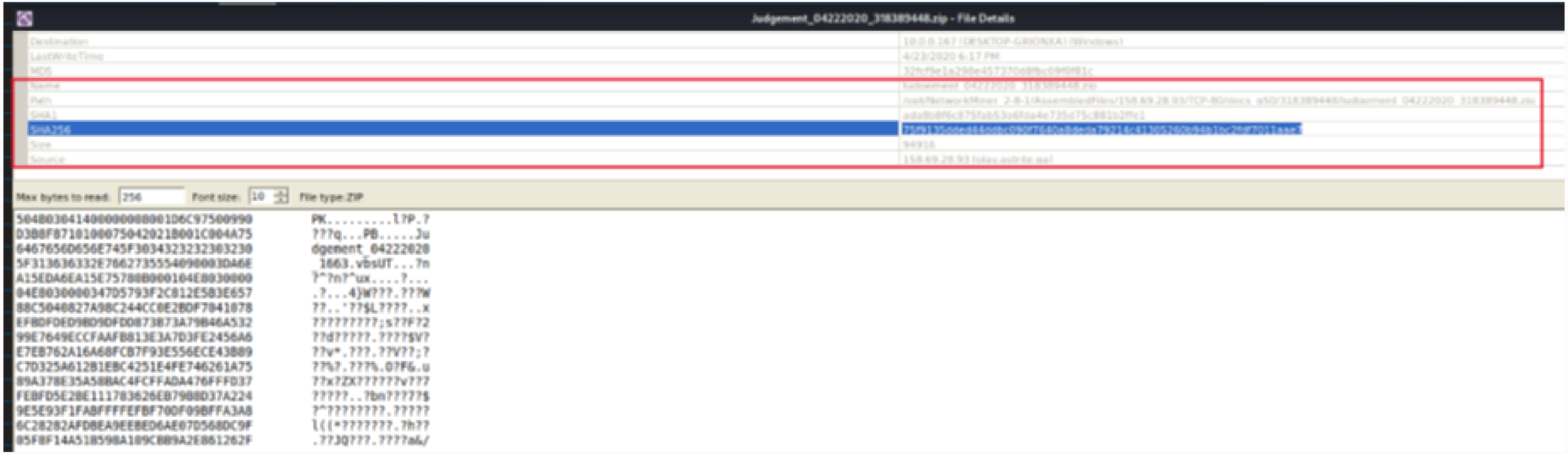
MD5	2cf20a1dd3693b996de4a559f1067850
SHA-1	6483bb40a7e3817f93a3ae95c6caea01715a4946
SHA-256	f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
Vhash	016046151d55520082z1700fb7z86z27050058fz
Authentihash	fdc38d6e4daa60a9f01f627fcd3bf41e5d577020b9e17a78f772f91da775b91c
Imphash	fe2ca1be3bda2a757036a89e54cc02db
SSDEEP	6144:ztKJnvON4sc6UKOahwyl2bbuBD9t4Piqqb5wVhFsbnN8ef:pKJnvON4sd7I1R9Ua5wVoz
TLSH	T16995C0AD447FC6F4F1932B708D485E6173ED8071293E8E8572BA243C14AF872675D2AB
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ 4.x (66.4%) | Win32 Executable MS Visual C++ (generic) (15.3%) | Win64 Executable (generic) (5.1%) | Win32 Dynamic Link Library (generic) (3.2%) | Win16 NE executable (generic) (2.4%)
DetectItEasy	PE32 | Linker: Polink (2.50*) [GUI32]
File size	1.86 MB (1950208 bytes)

Selain itu, kita juga dapat melihat detail-detail seperti hashing yang digunakan pada file CMSTP.EXE



4441	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.246.254 [t-9999.t-n
4447	msedge.net.cer	cer	2 542 B	13.107.42.254 [l-9999.l-ms
4447	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.42.254 [l-9999.l-ms
4452	www.linkedin.com.cer	cer	1 983 B	13.107.42.14 [l-0005.l-mse
4452	DigiCert SHA2 Secure Server.cer	cer	1 176 B	13.107.42.14 [l-0005.l-mse
4498	azurefd.us.cer	cer	1 583 B	20.140.56.69 [eafd-ffgov-s
4498	DigiCert SHA2 Secure Server.cer	cer	1 176 B	20.140.56.69 [eafd-ffgov-s
4564	footprintdns.com.cer	cer	2 177 B	94.245.88.12 [db3prdapp0
4564	Microsoft IT TLS CA 4.cer	cer	1 464 B	94.245.88.12 [db3prdapp0
4737	settings-win.data.microsoft[1].cer	cer	1 517 B	52.167.249.196 [settingsfd
4737	Microsoft Secure Server CA 2[1].cer	cer	1 756 B	52.167.249.196 [settingsfd
4817	Judgement_04222020_318389448.zip	zip	94 916 B	158.69.28.93 [play.astrite.c
4999	edge.skype.com.cer	cer	3 021 B	13.107.3.128 [s-0001.s-ms
4999	Microsoft IT TLS CA 4.cer	cer	1 464 B	13.107.3.128 [s-0001.s-ms
5455	8888.png.html	html	371 B	104.24.111.29 [atn24live.c
5464	suspendedpage.cgi.DB156929.html	html	7 774 B	104.24.111.29 [atn24live.c
5487	8888.png.html	html	380 B	220.158.200.181 [bg142.ca

Setelah melakukan pengecekan lebih dalam dengan networkminer dan wireshark, terdapat file .zip bernama “judgement_04222020_318389448.zip” yang diunduh oleh “elmer.obrien”



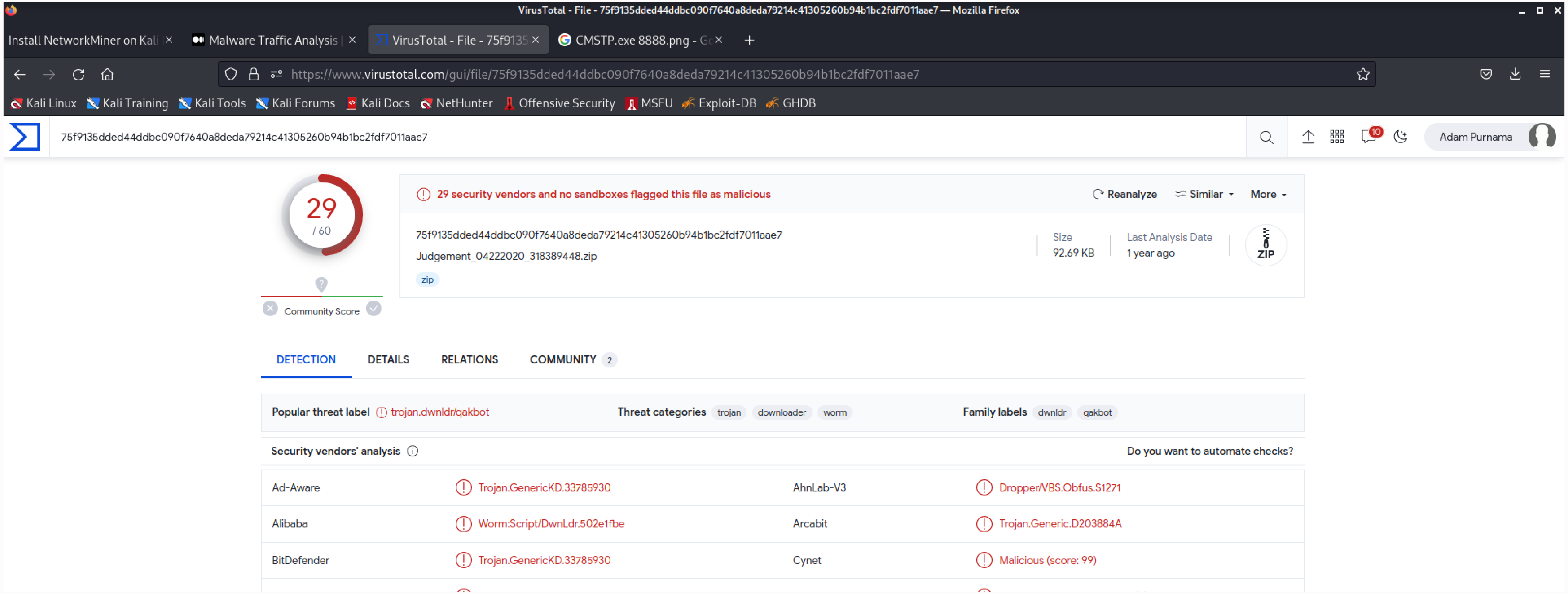
Judgement_04222020_318389448.zip - File Details

Destination	10.0.0.167 [DESKTOP-GRIONXA] (Windows)
LastWriteTime	4/23/2020 6:17 PM
MD5	32fcf9e1a298e457370d8fbc09f0f81c
Name	Judgement_04222020_318389448.zip
Path	/opt/NetworkMiner_2-8-1/AssembledFiles/158.69.28.93/TCP-80/docs_a50/318389448/Judgement_04222020_318389448.zip
SHA1	ada8b8f6c875fab53a6fda4e735d75c881b2ffc1
SHA256	75f9135ddedd44ddbc090f7640a8deda79214c413052600d94b1bc26df7011aae1
Size	94916
Source	158.69.28.93 [olav.astrito.pal]

Max bytes to read: 256 Font size: 10 File type:ZIP

```
504B0304140000000800 1D6C97500990        PK..........l?P.?
D3B8F8710100007504202 1B001C004A75       ???q....PB......Ju
6467656D656E745F3034323232303230         dgement_04222020
5F3136363332E7662735554090003D46E        _1663.vbsUT....?n
A15EDA6EA15E75788B000104E8030000         ?^?n?^ux.....?...
04E80300000347D5793F2C812E5B3E657        .?....4}W???.???W
88C5040827A98C244CC0E2BDF7041078         ??..'??$L????..x
EF8DFDED9BD9DFDD873B73A79B46A532         ??????????;s??F?2
99E7649ECCFAAFB813E3A7D3FE2456A6         ??d??????.????$V?
E7EB762A16A68FCB7F93E556ECE43B89         ??v*.???.??V??;?
C7D325A612B1EBC4251E4FE746261A75         ??%?.???%.O?F&.u
89A378E35A58BAC4FCFFADA476FFFD37         ??x?ZX???????v???
FEBFD5E2BE111783626EB79B8D37A224         ??????...?bn?????$
9E5E93F1FABFFFFEFBF70DF09BFFA3A8         ?^?????????.?????
6C28282AFDBEA9EEBED6AE07D568DC9F         l((*????????.?h??
05F8F14A518598A109C8B9A2E861262F         .??JQ???.????a&/
```

Disini dapat di lihat beberapa detail-detail yang ada pada zip file “judgement_04222020_318389448.zip” seperti nama file, hash, dan source.


VirusTotal - File - 75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7 — Mozilla Firefox
Install NetworkMiner on Kali
Malware Traffic Analysis |
VirusTotal - File - 75f9135
CMSTP.exe 8888.png - G
https://www.virustotal.com/gui/file/75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
Adam Purnama
29
/ 60
Community Score
Reanalyze
Similar
More
ZIP
DETECTION
DETAILS
RELATIONS
COMMUNITY 2

29 security vendors and no sandboxes flagged this file as malicious

75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
Judgement_04222020_318389448.zip
zip

Size 92.69 KB
Last Analysis Date 1 year ago

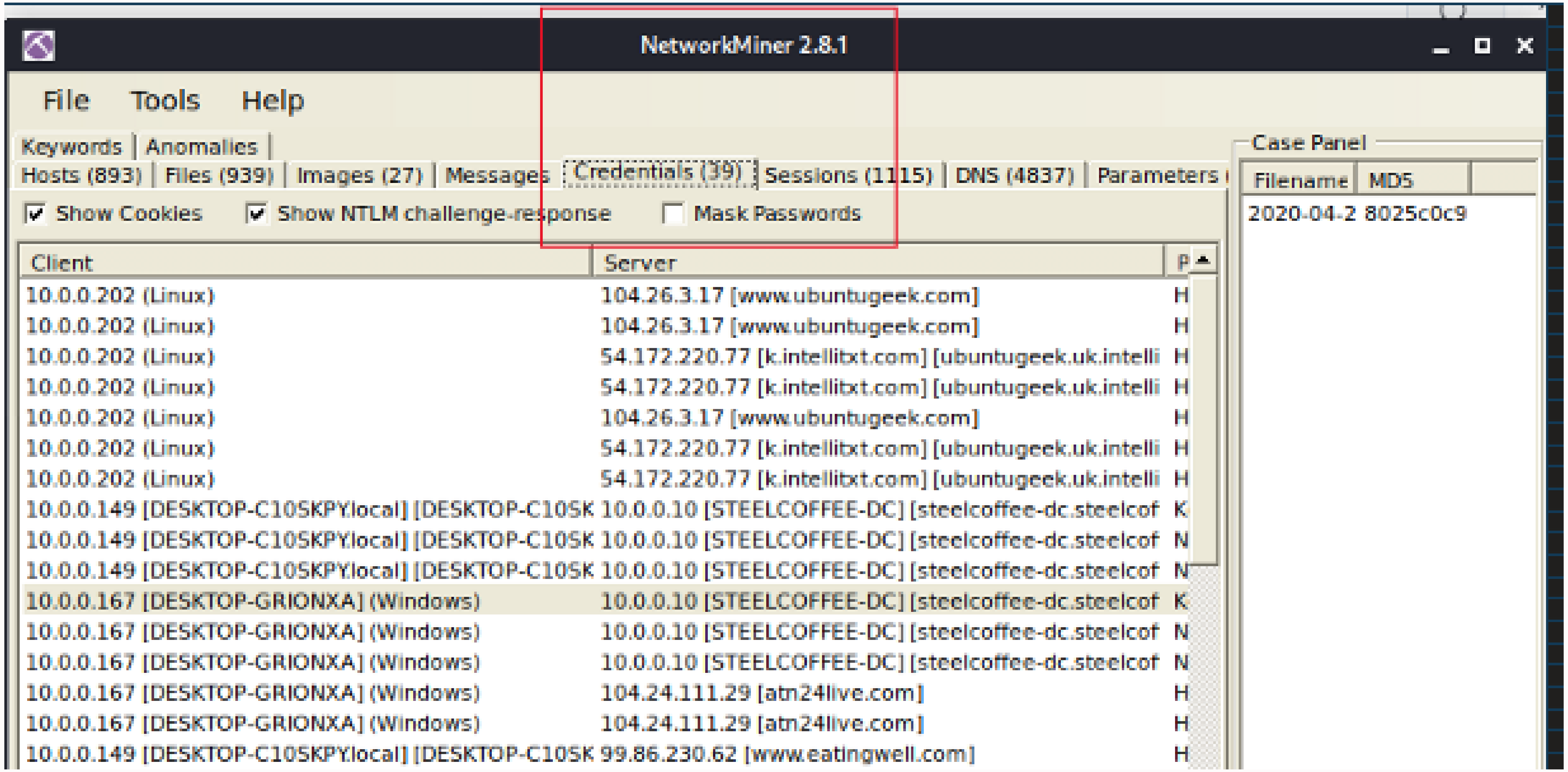
Popular threat label trojan.dwnldr/qakbot
Threat categories trojan downloader worm
Family labels dwnldr qakbot

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	Trojan.GenericKD.33785930	AhnLab-V3	Dropper/VBS.Obfus.S1271
Alibaba	Worm:Script/DwnLdr.502e1fbe	Arcabit	Trojan.Generic.D203884A
BitDefender	Trojan.GenericKD.33785930	Cynet	Malicious (score: 99)

Setelah itu, kita akan cek di Virus Total untuk melihat apakah file “judgement_04222020_318389448.zip” malicious atau tidak. Hasil pengecekan menunjukkan bahwa tingkat maliciousnya sebesar 29/60 dan juga threat labelnya adalah trojan.dwnldr/qakbot. dalam zip terdapat juga script .vbs dan ketika script tersebut berjalan akan redirect ke sebuah domain untuk mendownload payload “8888.png” yang dimana .png tersebut malicious.

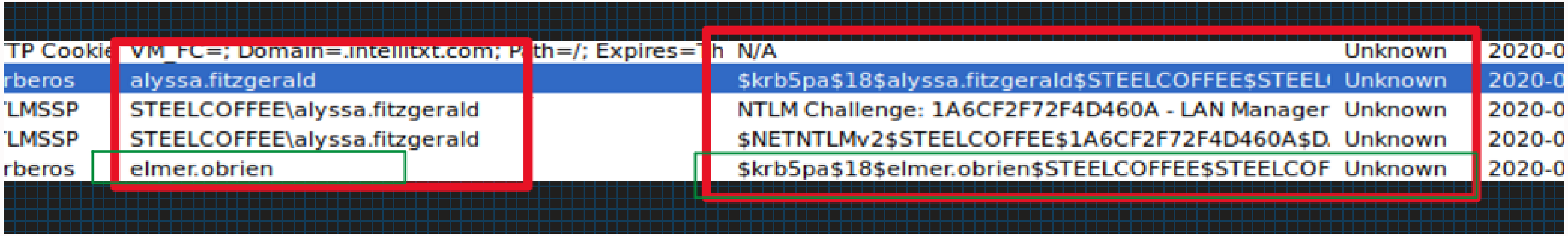


☑ Show Cookies ☑ Show NTLM challenge-response ☐ Mask Passwords

Client	Server	P
10.0.0.202 (Linux)	104.26.3.17 [www.ubuntugeek.com]	H
10.0.0.202 (Linux)	104.26.3.17 [www.ubuntugeek.com]	H
10.0.0.202 (Linux)	54.172.220.77 [k.intellitxt.com] [ubuntugeek.uk.intelli	H
10.0.0.202 (Linux)	54.172.220.77 [k.intellitxt.com] [ubuntugeek.uk.intelli	H
10.0.0.202 (Linux)	104.26.3.17 [www.ubuntugeek.com]	H
10.0.0.202 (Linux)	54.172.220.77 [k.intellitxt.com] [ubuntugeek.uk.intelli	H
10.0.0.202 (Linux)	54.172.220.77 [k.intellitxt.com] [ubuntugeek.uk.intelli	H
10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SK	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	K
10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SK	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	N
10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SK	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	N
10.0.0.167 [DESKTOP-GRIONXA] (Windows)	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	K
10.0.0.167 [DESKTOP-GRIONXA] (Windows)	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	N
10.0.0.167 [DESKTOP-GRIONXA] (Windows)	10.0.0.10 [STEELCOFFEE-DC] [steelcoffee-dc.steelcof	N
10.0.0.167 [DESKTOP-GRIONXA] (Windows)	104.24.111.29 [atn24live.com]	H
10.0.0.167 [DESKTOP-GRIONXA] (Windows)	104.24.111.29 [atn24live.com]	H
10.0.0.149 [DESKTOP-C10SKPY.local] [DESKTOP-C10SK	99.86.230.62 [www.eatingwell.com]	H

Filename	MD5
2020-04-2	8025c0c9

Selanjutnya, di networkminer nya terdapat 39 list credential yang tersimpan di dalam log pcap tersebut.



TP Cookie	VM_FC=; Domain=.intellitxt.com; Path=/; Expires=Th	N/A	Unknown	2020-0
rberos	alyssa.fitzgerald	$krb5pa$18$alyssa.fitzgerald$STEELCOFFEE$STEEL	Unknown	2020-0
LMSSP	STEELCOFFEE\alyssa.fitzgerald	NTLM Challenge: 1A6CF2F72F4D460A - LAN Manager	Unknown	2020-0
LMSSP	STEELCOFFEE\alyssa.fitzgerald	$NETNTLMv2$STEELCOFFEE$1A6CF2F72F4D460A$D	Unknown	2020-0
rberos	elmer.obrien	$krb5pa$18$elmer.obrien$STEELCOFFEE$STEELCOF	Unknown	2020-0

jika dilihat, terdapat hash MD5 dari host yang telah melakukan input password, yaitu ada alyzza.fitzgerald dan elmer.obrien

thankyou