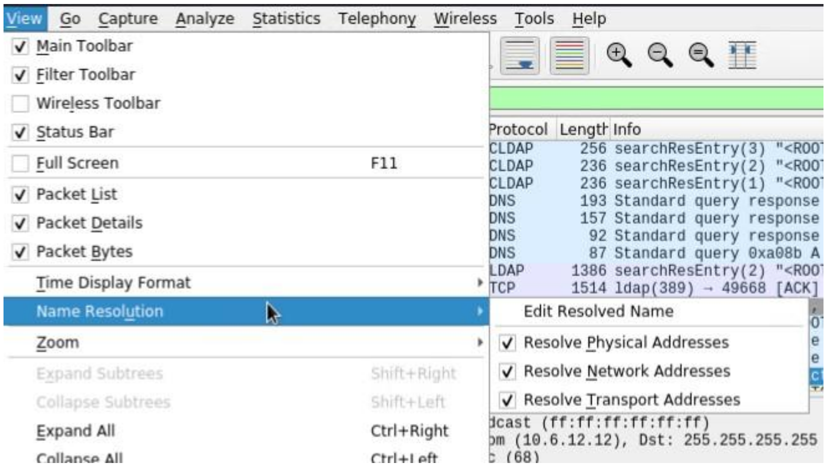
Network Forensic Analysis Report

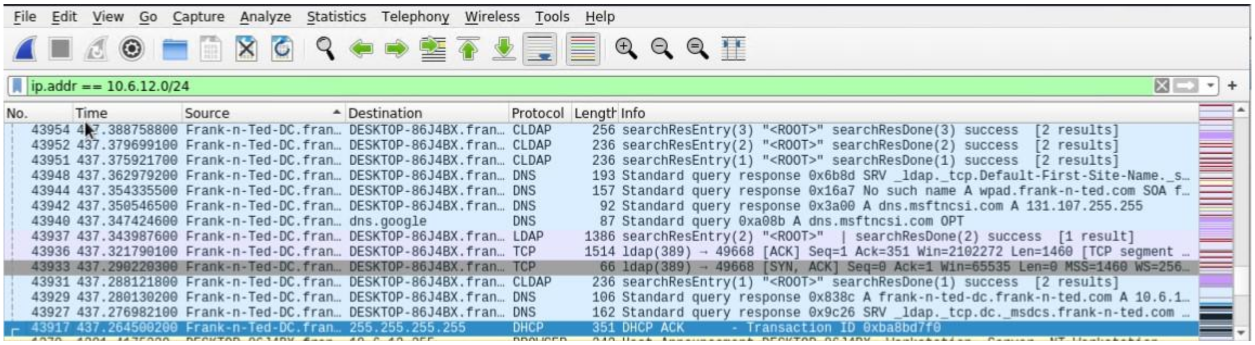
Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
   `Frank-n-Ted-DC.frank-n-ted.com`



```
Protocol Length Info
CLDAP      256 searchResEntry(3) "<ROOT
CLDAP      236 searchResEntry(2) "<ROOT
CLDAP      236 searchResEntry(1) "<ROOT
DNS        193 Standard query response
DNS        157 Standard query response
DNS         92 Standard query response
DNS         87 Standard query 0xa08b A
LDAP      1386 searchResEntry(2) "<ROOT
TCP       1514 ldap(389) → 49668 [ACK]
dcast (ff:ff:ff:ff:ff:ff)
om (10.6.12.12), Dst: 255.255.255.255
c (68)
```

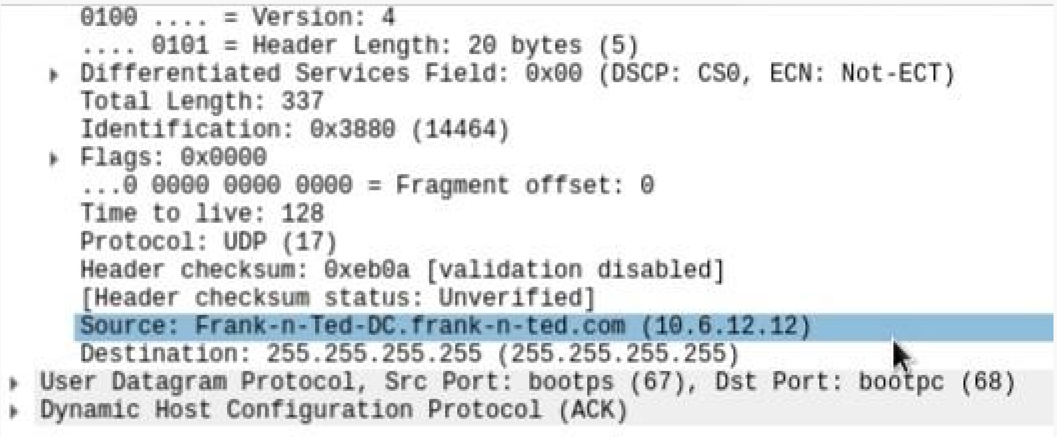


```
ip.addr == 10.6.12.0/24
```

```
No.   Time          Source              Destination         Protocol Length Info
43954 437.388758800 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… CLDAP     256 searchResEntry(3) "<ROOT>" searchResDone(3) success  [2 results]
43952 437.379699100 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… CLDAP     236 searchResEntry(2) "<ROOT>" searchResDone(2) success  [2 results]
43951 437.375921700 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… CLDAP     236 searchResEntry(1) "<ROOT>" searchResDone(1) success  [2 results]
43948 437.362979200 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS       193 Standard query response 0x6b8d SRV _ldap._tcp.Default-First-Site-Name._s…
43944 437.354335500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS       157 Standard query response 0x16a7 No such name A wpad.frank-n-ted.com SOA f…
43942 437.350546500 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS        92 Standard query response 0x3a00 A dns.msftncsi.com A 131.107.255.255
43940 437.347424600 Frank-n-Ted-DC.fran… dns.google           DNS        87 Standard query 0xa08b A dns.msftncsi.com OPT
43937 437.343987600 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… LDAP     1386 searchResEntry(2) "<ROOT>"  | searchResDone(2) success  [1 result]
43936 437.321790100 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… TCP      1514 ldap(389) → 49668 [ACK] Seq=1 Ack=351 Win=2102272 Len=1460 [TCP segment …
43933 437.290220300 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… TCP        66 ldap(389) → 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256…
43931 437.288121800 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… CLDAP     236 searchResEntry(1) "<ROOT>" searchResDone(1) success  [2 results]
43929 437.280130200 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS       106 Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com A 10.6.1…
43927 437.276982100 Frank-n-Ted-DC.fran… DESKTOP-86J4BX.fran… DNS       162 Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com …
43917 437.264500200 Frank-n-Ted-DC.fran… 255.255.255.255      DHCP      351 DHCP ACK      - Transaction ID 0xba8bd7f0
```

2. What is the IP address of the Domain Controller (DC) of the AD network?

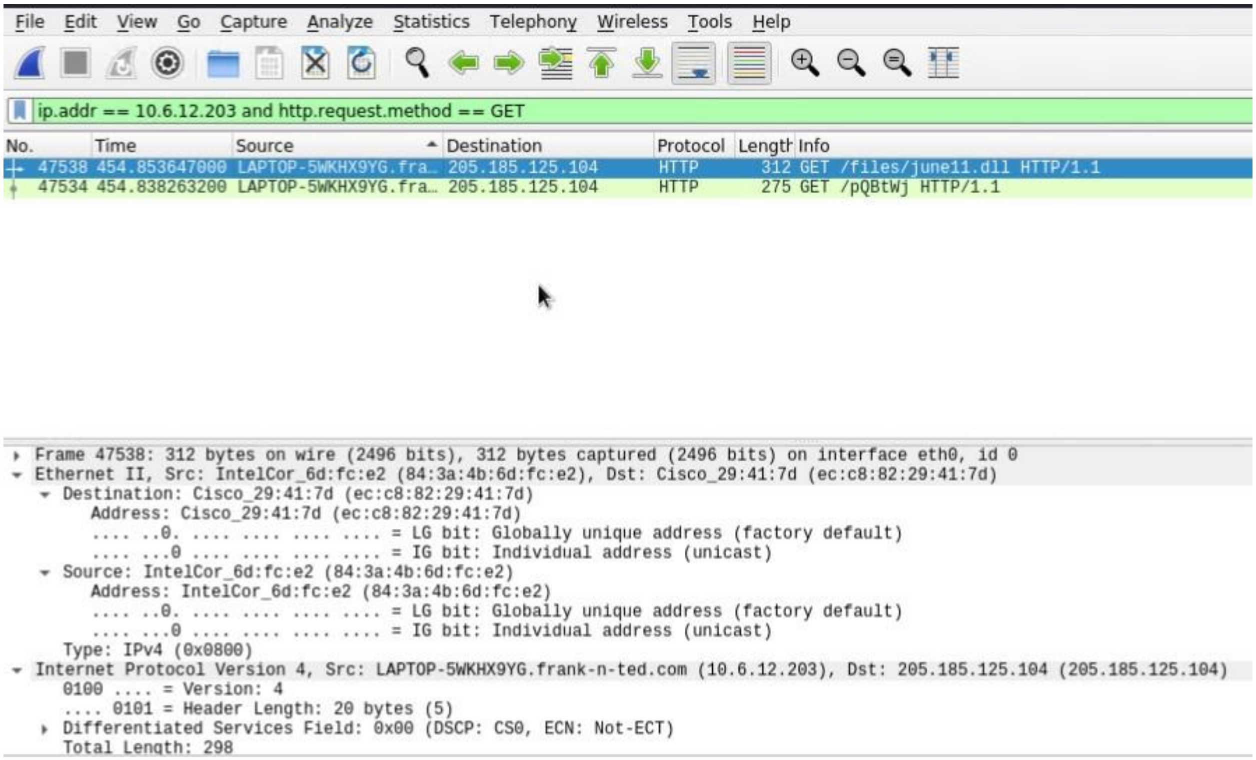
```
10.6.12.12
```



```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 337
      Identification: 0x3880 (14464)
    ▸ Flags: 0x0000
      ...0 0000 0000 0000 = Fragment offset: 0
      Time to live: 128
      Protocol: UDP (17)
      Header checksum: 0xeb0a [validation disabled]
      [Header checksum status: Unverified]
      Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
      Destination: 255.255.255.255 (255.255.255.255)
▸ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▸ Dynamic Host Configuration Protocol (ACK)
```

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

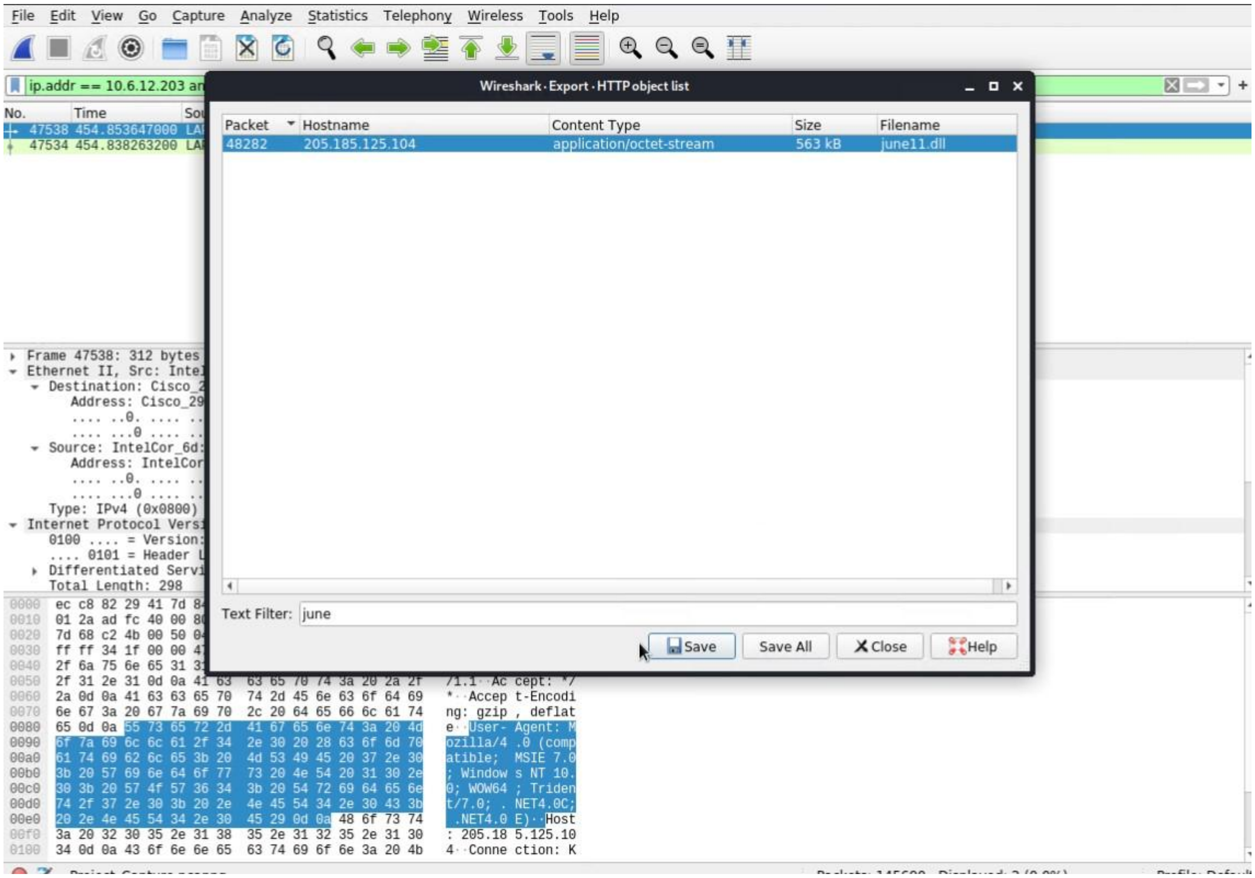
```
june11.dll
```



```
ip.addr == 10.6.12.203 and http.request.method == GET
```

```
No.    Time              Source                  Destination      Protocol  Length Info
47538  454.853647000     LAPTOP-5WKHX9YG.fra…    205.185.125.104  HTTP      312 GET /files/june11.dll HTTP/1.1
47534  454.838263200     LAPTOP-5WKHX9YG.fra…    205.185.125.104  HTTP      275 GET /pQBtWj HTTP/1.1
```

```
▸ Frame 47538: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
▾ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
  ▾ Destination: Cisco_29:41:7d (ec:c8:82:29:41:7d)
      Address: Cisco_29:41:7d (ec:c8:82:29:41:7d)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
      Address: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 298
```



```
ip.addr == 10.6.12.203 an
No.   Time                Sou
47538 454.853647000 LA
47534 454.838263200 LA
```

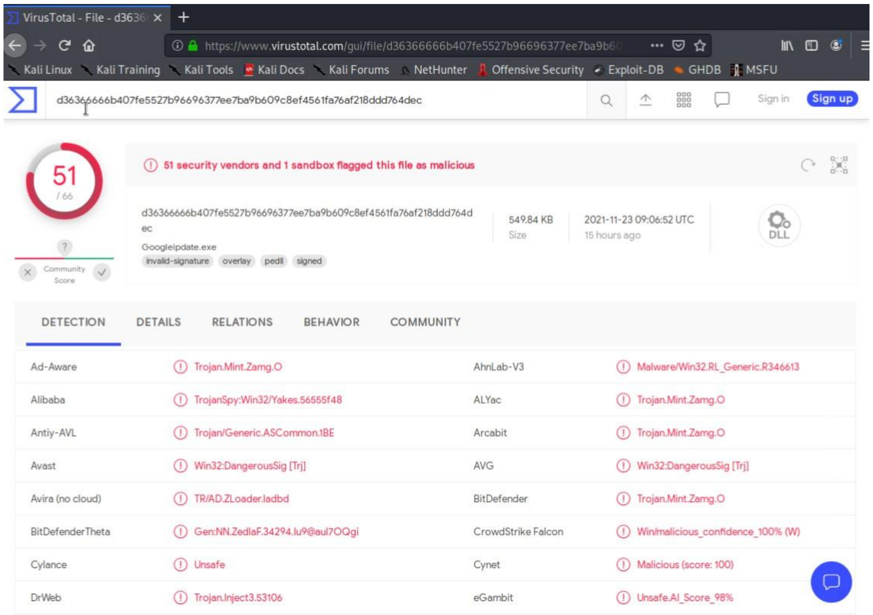
Packet	Hostname	Content Type	Size	Filename
48282	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: june

```
▸ Frame 47538: 312 bytes
▾ Ethernet II, Src: Intel
  ▾ Destination: Cisco_2
      Address: Cisco_29
      .... ..0. .... ..
      .... ...0 .... ..
  ▾ Source: IntelCor_6d
      Address: IntelCor
      .... ..0. .... ..
      .... ...0 .... ..
    Type: IPv4 (0x0800)
▾ Internet Protocol Versi
    0100 .... = Version:
    .... 0101 = Header L
  ▸ Differentiated Servi
    Total Length: 298
```

```
0000  ec c8 82 29 41 7d 84
0010  01 2a ad fc 40 00 80
0020  7d 68 c2 4b 00 50 04
0030  ff ff 34 1f 00 00 47
0040  2f 6a 75 6e 65 31 31
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10.
00c0  30 3b 20 57 4f 57 36 34  3b 20 54 72 69 64 65 6e   0; WOW64 ; Triden
00d0  74 2f 37 2e 30 3b 20 2e  4e 45 54 34 2e 30 43 3b   t/7.0; . NET4.0C;
00e0  20 2e 4e 45 54 34 2e 30  45 29 0d 0a 48 6f 73 74    .NET4.0 E)··Host
00f0  3a 20 32 30 35 2e 31 38  35 2e 31 32 35 2e 31 30   : 205.18 5.125.10
0100  34 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   4··Conne ction: K
```

4. Upload the file to VirusTotal.com.



https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b60

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

51 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleipdate.exe

invalid-signature overlay pedll signed

549.84 KB
Size

2021-11-23 09:06:52 UTC
15 hours ago

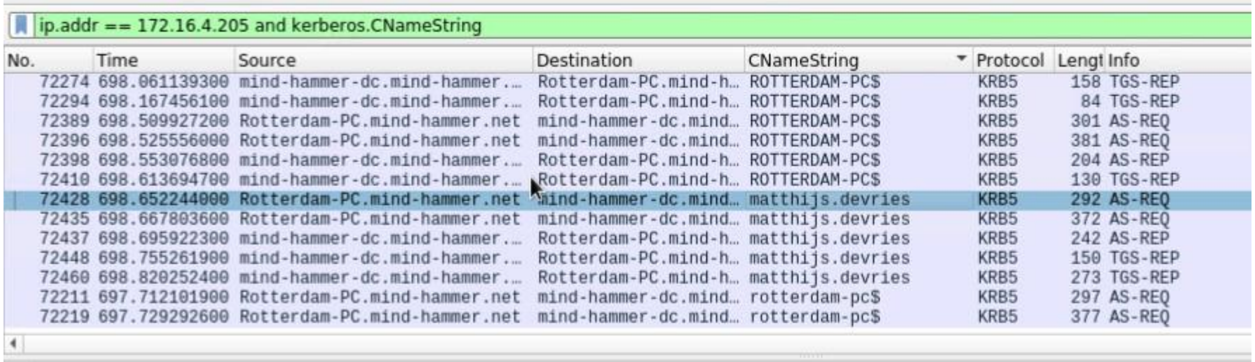
Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.56555f48	ALYac	Trojan.Mint.Zamg.O
Antiy-AVL	Trojan/Generic.ASCommon.1BE	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34294.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Inject3.53106	eGambit	Unsafe.AI_Score_98%

5. What kind of malware is this classified as?

   trojan.malware

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:
   - Host name: `Rotterdam-PC.mind-hammer.net`
   - IP address: `172.16.4.205`
   - MAC address: `LenovoEM_b0:64:a4 (00:59:07:b0:63:a4)`
2. What is the username of the Windows user whose computer is infected?

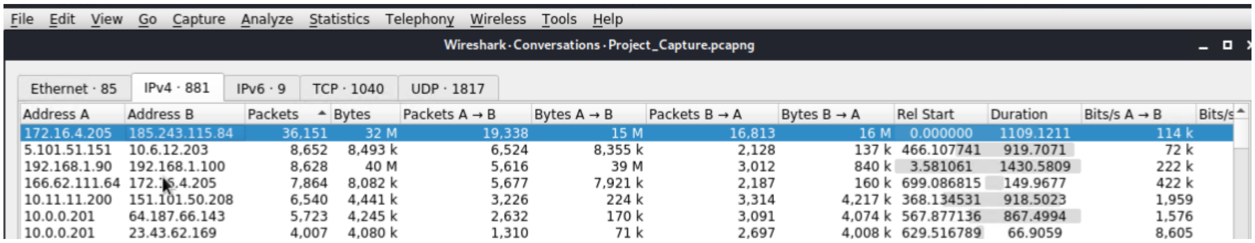


ip.addr == 172.16.4.205 and kerberos.CNameString

No.	Time	Source	Destination	CNameString	Protocol	Lengt	Info
72274	698.061139300	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	ROTTERDAM-PC$	KRB5	158	TGS-REP
72294	698.167456100	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	ROTTERDAM-PC$	KRB5	84	TGS-REP
72389	698.509927200	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	ROTTERDAM-PC$	KRB5	301	AS-REQ
72396	698.525556000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	ROTTERDAM-PC$	KRB5	381	AS-REQ
72398	698.553076800	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	ROTTERDAM-PC$	KRB5	204	AS-REP
72410	698.613694700	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	ROTTERDAM-PC$	KRB5	130	TGS-REP
72428	698.652244000	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	matthijs.devries	KRB5	292	AS-REQ
72435	698.667803600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	matthijs.devries	KRB5	372	AS-REQ
72437	698.695922300	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	matthijs.devries	KRB5	242	AS-REP
72448	698.755261900	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	matthijs.devries	KRB5	150	TGS-REP
72460	698.820252400	mind-hammer-dc.mind-hammer.…	Rotterdam-PC.mind-h…	matthijs.devries	KRB5	273	TGS-REP
72211	697.712101900	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	rotterdam-pc$	KRB5	297	AS-REQ
72219	697.729292600	Rotterdam-PC.mind-hammer.net	mind-hammer-dc.mind…	rotterdam-pc$	KRB5	377	AS-REQ

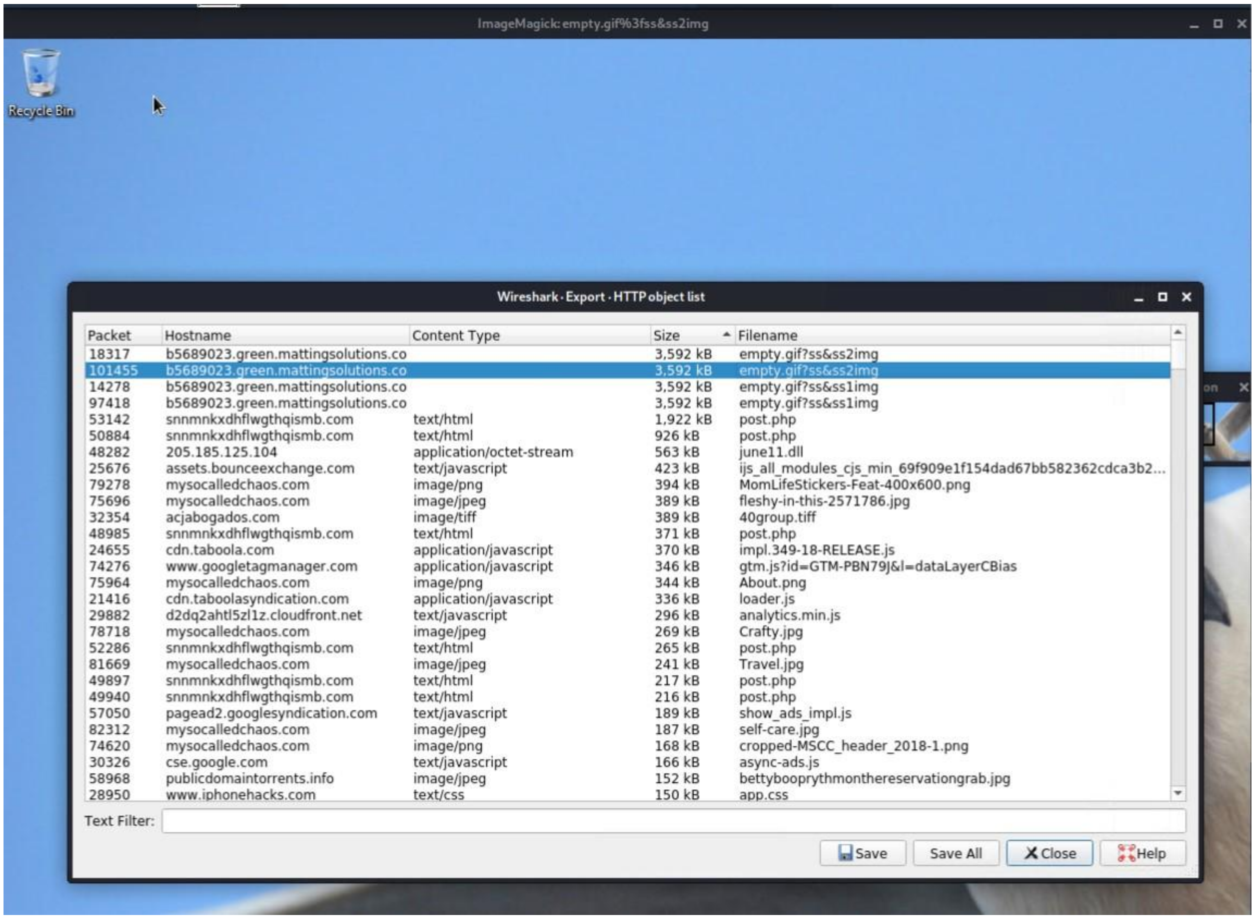
```
matthijs.devries
```

3. What are the IP addresses used in the actual infection traffic? `185.243.115.84`

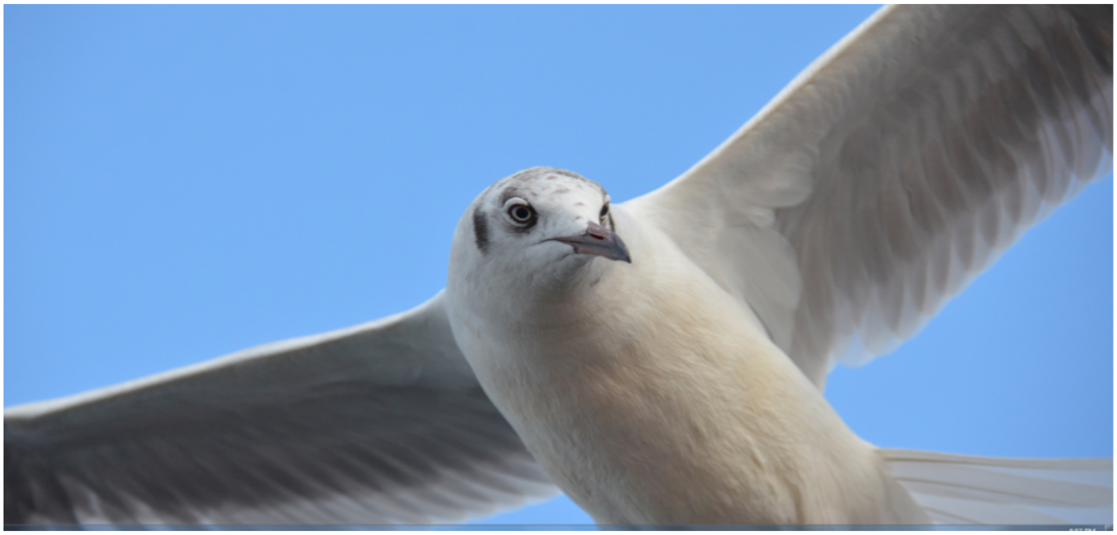

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · Project_Capture.pcapng
Ethernet · 85
IPv4 · 881
IPv6 · 9
TCP · 1040
UDP · 1817

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s
172.16.4.205	185.243.115.84	36,151	32 M	19,338	15 M	16,813	16 M	0.000000	1109.1211	114 k	
5.101.51.151	10.6.12.203	8,652	8,493 k	6,524	8,355 k	2,128	137 k	466.107741	919.7071	72 k	
192.168.1.90	192.168.1.100	8,628	40 M	5,616	39 M	3,012	840 k	3.581061	1430.5809	222 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	699.086815	149.9677	422 k	
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	368.134531	918.5023	1,959	
10.0.0.201	64.187.66.143	5,723	4,245 k	2,632	170 k	3,091	4,074 k	567.877136	867.4994	1,576	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	629.516789	66.9059	8,605	

4. As a bonus, retrieve the desktop background of the Windows host.

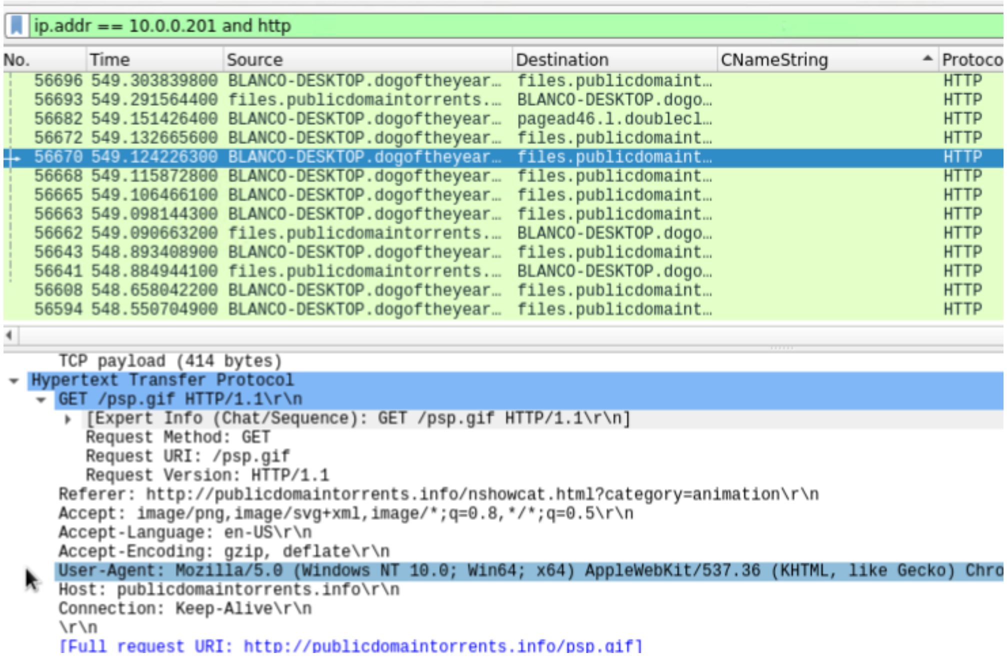

ImageMagick: empty.gif%3fss&ss2img
Recycle Bin
Wireshark · Export · HTTP object list
Text Filter:
Save
Save All
Close
Help

Packet	Hostname	Content Type	Size	Filename
18317	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
101455	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2img
14278	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
97418	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1img
53142	snnmnkxdhflwgthqismb.com	text/html	1,922 kB	post.php
50884	snnmnkxdhflwgthqismb.com	text/html	926 kB	post.php
48282	205.185.125.104	application/octet-stream	563 kB	june11.dll
25676	assets.bounceexchange.com	text/javascript	423 kB	ijs_all_modules_cjs_min_69f909e1f154dad67bb582362cdca3b2…
79278	mysocalledchaos.com	image/png	394 kB	MomLifeStickers-Feat-400x600.png
75696	mysocalledchaos.com	image/jpeg	389 kB	fleshy-in-this-2571786.jpg
32354	acjabogados.com	image/tiff	389 kB	40group.tiff
48985	snnmnkxdhflwgthqismb.com	text/html	371 kB	post.php
24655	cdn.taboola.com	application/javascript	370 kB	impl.349-18-RELEASE.js
74276	www.googletagmanager.com	application/javascript	346 kB	gtm.js?id=GTM-PBN79J&l=dataLayerCBias
75964	mysocalledchaos.com	image/png	344 kB	About.png
21416	cdn.taboolasyndication.com	application/javascript	336 kB	loader.js
29882	d2dq2ahtl5zl1z.cloudfront.net	text/javascript	296 kB	analytics.min.js
78718	mysocalledchaos.com	image/jpeg	269 kB	Crafty.jpg
52286	snnmnkxdhflwgthqismb.com	text/html	265 kB	post.php
81669	mysocalledchaos.com	image/jpeg	241 kB	Travel.jpg
49897	snnmnkxdhflwgthqismb.com	text/html	217 kB	post.php
49940	snnmnkxdhflwgthqismb.com	text/html	216 kB	post.php
57050	pagead2.googlesyndication.com	text/javascript	189 kB	show_ads_impl.js
82312	mysocalledchaos.com	image/jpeg	187 kB	self-care.jpg
74620	mysocalledchaos.com	image/png	168 kB	cropped-MSCC_header_2018-1.png
30326	cse.google.com	text/javascript	166 kB	async-ads.js
58968	publicdomaintorrents.info	image/jpeg	152 kB	bettybooprythmonthereservationgrab.jpg
28950	www.iphonehacks.com	text/css	150 kB	app.css



Illegal Downloads

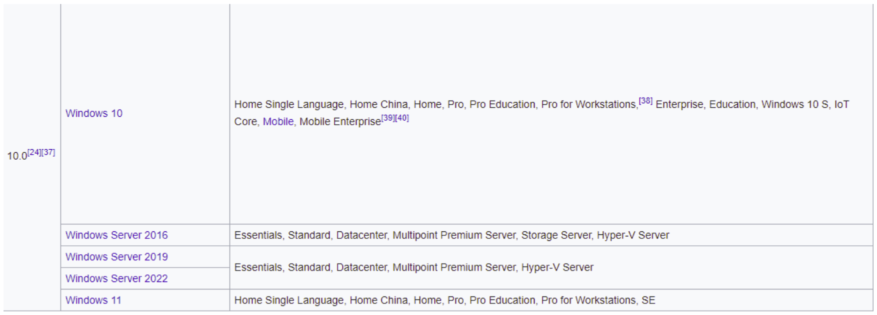
1. Find the following information about the machine with IP address `10.0.0.201`:
   - MAC address: `Msi_18:66:c8 (00:16:17:18.66:c8)`
   - Windows username: `elmer.blanco`
   - OS version: `Windows NT 10.0`



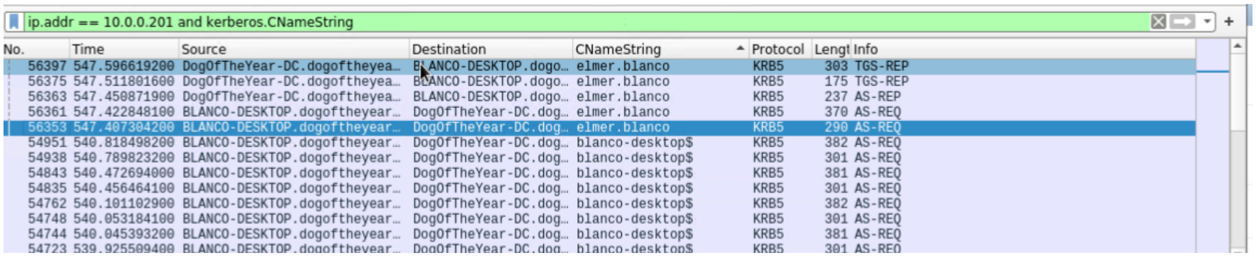
ip.addr == 10.0.0.201 and http

```
No.   Time           Source                         Destination              CNameString   Protoco
56696 549.303839800  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56693 549.291564400  files.publicdomaintorrents.…   BLANCO-DESKTOP.dogo…                   HTTP
56682 549.151426400  BLANCO-DESKTOP.dogoftheyear…   pagead46.l.doublecl…                   HTTP
56672 549.132665600  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56670 549.124226300  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56668 549.115872800  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56665 549.106466100  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56663 549.098144300  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56662 549.090663200  files.publicdomaintorrents.…   BLANCO-DESKTOP.dogo…                   HTTP
56643 548.893408900  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56641 548.884944100  files.publicdomaintorrents.…   BLANCO-DESKTOP.dogo…                   HTTP
56608 548.658042200  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
56594 548.550704900  BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                   HTTP
```

```
    TCP payload (414 bytes)
Hypertext Transfer Protocol
    GET /psp.gif HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /psp.gif HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /psp.gif
        Request Version: HTTP/1.1
    Referer: http://publicdomaintorrents.info/nshowcat.html?category=animation\r\n
    Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
    Accept-Language: en-US\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
    Host: publicdomaintorrents.info\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://publicdomaintorrents.info/psp.gif]
```



10.0[24][37]	Windows 10	Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations,[38] Enterprise, Education, Windows 10 S, IoT Core, Mobile, Mobile Enterprise[39][40]
	Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
	Windows Server 2019	Essentials, Standard, Datacenter, Multipoint Premium Server, Hyper-V Server
	Windows Server 2022	
	Windows 11	Home Single Language, Home China, Home, Pro, Pro Education, Pro for Workstations, SE

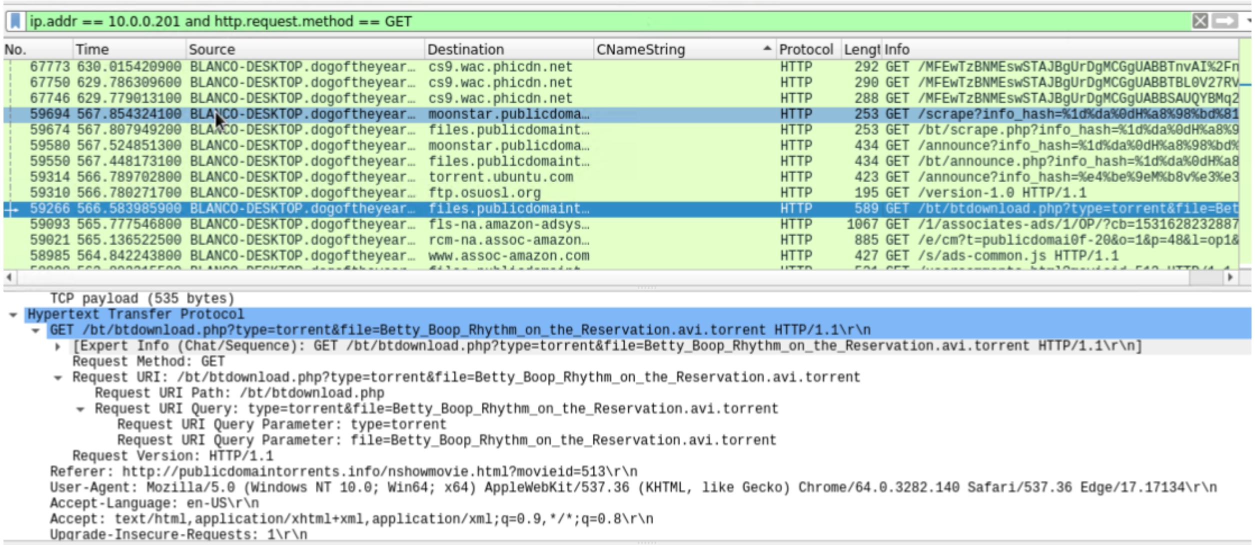


ip.addr == 10.0.0.201 and kerberos.CNameString

```
No.   Time           Source                         Destination           CNameString      Protocol Lengt Info
56397 547.596619200  DogOfTheYear-DC.dogoftheyea…   BLANCO-DESKTOP.dogo…  elmer.blanco     KRB5     303 TGS-REP
56375 547.511801600  DogOfTheYear-DC.dogoftheyea…   BLANCO-DESKTOP.dogo…  elmer.blanco     KRB5     175 TGS-REP
56363 547.450871900  DogOfTheYear-DC.dogoftheyea…   BLANCO-DESKTOP.dogo…  elmer.blanco     KRB5     237 AS-REP
56361 547.422848100  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  elmer.blanco     KRB5     370 AS-REQ
56353 547.407304200  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  elmer.blanco     KRB5     290 AS-REQ
54951 540.818498200  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     382 AS-REQ
54938 540.789823200  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     301 AS-REQ
54843 540.472694000  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     381 AS-REQ
54835 540.456464100  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     301 AS-REQ
54762 540.101102900  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     382 AS-REQ
54748 540.053184100  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     301 AS-REQ
54744 540.045393200  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     381 AS-REQ
54723 539.925509400  BLANCO-DESKTOP.dogoftheyear…   DogOfTheYear-DC.dog…  blanco-desktop$  KRB5     301 AS-REQ
```

2. Which torrent file did the user download?

```
Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
```



```
ip.addr == 10.0.0.201 and http.request.method == GET

No.   Time          Source                          Destination               CNameString   Protocol Lengt Info
67773 630.015420900 BLANCO-DESKTOP.dogoftheyear…   cs9.wac.phicdn.net                      HTTP      292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTnvAI%2Fn
67750 629.786309600 BLANCO-DESKTOP.dogoftheyear…   cs9.wac.phicdn.net                      HTTP      290 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RV
67746 629.779013100 BLANCO-DESKTOP.dogoftheyear…   cs9.wac.phicdn.net                      HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2
59694 567.854324100 BLANCO-DESKTOP.dogoftheyear…   moonstar.publicdoma…                    HTTP      253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81
59674 567.807949200 BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                    HTTP      253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%9
59580 567.524851300 BLANCO-DESKTOP.dogoftheyear…   moonstar.publicdoma…                    HTTP      434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%
59550 567.448173100 BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                    HTTP      434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8
59314 566.789702800 BLANCO-DESKTOP.dogoftheyear…   torrent.ubuntu.com                      HTTP      423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3
59310 566.780271700 BLANCO-DESKTOP.dogoftheyear…   ftp.osuosl.org                          HTTP      195 GET /version-1.0 HTTP/1.1
59266 566.583985900 BLANCO-DESKTOP.dogoftheyear…   files.publicdomaint…                    HTTP      589 GET /bt/btdownload.php?type=torrent&file=Bet
59093 565.777546800 BLANCO-DESKTOP.dogoftheyear…   fls-na.amazon-adsys…                    HTTP     1067 GET /1/associates-ads/1/OP/?cb=1531628232887
59021 565.136522500 BLANCO-DESKTOP.dogoftheyear…   rcm-na.assoc-amazon…                    HTTP      885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&
58985 564.842243800 BLANCO-DESKTOP.dogoftheyear…   www.assoc-amazon.com                    HTTP      427 GET /s/ads-common.js HTTP/1.1

    TCP payload (535 bytes)
  Hypertext Transfer Protocol
    GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        Request URI Path: /bt/btdownload.php
        Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
          Request URI Query Parameter: type=torrent
          Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request Version: HTTP/1.1
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
```