

No.	Time	Source	Destination	Protocol	Length	Info
3	2018-10-17 16:36:31.836352	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xbfb8
A	www.mit.edu					
Frame 3:	79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0					
Interface id:	0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})					
Interface name:	\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}					
Encapsulation type:	Ethernet (1)					
Arrival Time:	Oct 17, 2018 16:36:31.836352000 中国标准时间					
[Time shift for this packet:	0.000000000 seconds]					
Epoch Time:	1539765391.836352000 seconds					
[Time delta from previous captured frame:	0.591418000 seconds]					
[Time delta from previous displayed frame:	0.000000000 seconds]					
[Time since reference or first frame:	1.592885000 seconds]					
Frame Number:	3					
Frame Length:	79 bytes (632 bits)					
Capture Length:	79 bytes (632 bits)					
[Frame is marked:	False]					
[Frame is ignored:	False]					
[Protocols in frame:	eth:ethertype:pppoes:ppp:ip:udp:dns]					
[Coloring Rule Name:	UDP]					
[Coloring Rule String:	udp]					
Ethernet II, Src:	AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)	Dst:	HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)			
Destination:	HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)					
Address:	HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)					
.... .0. =	LG bit: Globally unique address (factory default)					
.... .0. =	IG bit: Individual address (unicast)					
Source:	AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)					
Address:	AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)					
.... .0. =	LG bit: Globally unique address (factory default)					
.... .0. =	IG bit: Individual address (unicast)					
Type:	PPPoE Session (0x8864)					
PPP-over-Ethernet Session						
0001 =	Version: 1					
.... 0001 =	Type: 1					
Code:	Session Data (0x00)					
Session ID:	0x629d					
Payload Length:	59					
Point-to-Point Protocol						
Protocol:	Internet Protocol version 4 (0x0021)					
Internet Protocol Version 4, Src:	10.173.88.157, Dst:	202.117.112.3				
0100 =	Version: 4					
.... 0101 =	Header Length: 20 bytes (5)					
Differentiated Services Field:	0x00 (DSCP: CS0, ECN: Not-ECT)					
0000 00.. =	Differentiated Services Codepoint: Default (0)					
.... ..00 =	Explicit Congestion Notification: Not ECN-Capable Transport (0)					
Total Length:	57					
Identification:	0x37c6 (14278)					
Flags:	0x0000					
0... =	Reserved bit: Not set					
.0... =	Don't fragment: Not set					
..0. =	More fragments: Not set					
...0 0000 0000 0000 =	Fragment offset: 0					
Time to live:	64					
Protocol:	UDP (17)					
Header checksum:	0xa52b [validation disabled]					
[Header checksum status:	Unverified]					
Source:	10.173.88.157					
Destination:	202.117.112.3					
User Datagram Protocol, Src Port:	55223, Dst Port:	53				
Source Port:	55223					
Destination Port:	53					
Length:	37					
Checksum:	0x7790 [unverified]					
[Checksum Status:	Unverified]					
[Stream index:	1]					
Domain Name System (query)						
Transaction ID:	0xbfb8					
Flags:	0x0100 Standard query					
0... =	Response: Message is a query					
.000 0... =	Opcode: Standard query (0)					
.... .0. =	Truncated: Message is not truncated					
.... .1 =	Recursion desired: Do query recursively					
....0. =	Z: reserved (0)					
....0 =	Non-authenticated data: Unacceptable					
Questions:	1					
Answer RRs:	0					
Authority RRs:	0					

Additional RRs: 0
Queries

www.mit.edu: type A, class IN
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 10]

No.	Time	Source	Destination	Protocol	Length	Info
4	2018-10-17 16:36:31.864942	10.173.88.157	218.30.19.40	DNS	79	Standard query 0xbfb8

A www.mit.edu
Frame 4: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.864942000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.864942000 seconds
[Time delta from previous captured frame: 0.028590000 seconds]
[Time delta from previous displayed frame: 0.028590000 seconds]
[Time since reference or first frame: 1.621475000 seconds]
Frame Number: 4
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x626c (25196)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7b7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 55223, Dst Port: 53
Source Port: 55223
Destination Port: 53
Length: 37
Checksum: 0xc4c2 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Domain Name System (query)
Transaction ID: 0xbfb8
Flags: 0x0100 Standard query

0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 5]

No.	Time	Source	Destination	Protocol	Length	Info
5	2018-10-17 16:36:31.944316	218.30.19.40	10.173.88.157	DNS	168	Standard query response

Frame 5: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.944316000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.944316000 seconds
[Time delta from previous captured frame: 0.079374000 seconds]
[Time delta from previous displayed frame: 0.079374000 seconds]
[Time since reference or first frame: 1.700849000 seconds]
Frame Number: 5
Frame Length: 168 bytes (1344 bits)
Capture Length: 168 bytes (1344 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 148
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 146
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1... = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0ca [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55223

Source Port: 53
Destination Port: 55223
Length: 126
Checksum: 0xb33f [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Domain Name System (response)
Transaction ID: 0xbfb8
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0... = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 Name: www.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 25
 CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 Name: www.mit.edu.edgekey.net
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 24
 CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.2.132.180
 Name: e9566.dscb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 4
 Address: 23.2.132.180
[Request In: 4]
[Time: 0.079374000 seconds]
No. Time Source Destination Protocol Length Info
7 2018-10-17 16:36:31.948005 10.173.88.157 202.117.112.3 DNS 93 Standard query 0xe32a
A e9566.dscb.akamaiedge.net
Frame 7: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.948005000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.948005000 seconds
[Time delta from previous captured frame: 0.001102000 seconds]
[Time delta from previous displayed frame: 0.003689000 seconds]
[Time since reference or first frame: 1.704538000 seconds]
Frame Number: 7
Frame Length: 93 bytes (744 bits)
Capture Length: 93 bytes (744 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 73

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 71
Identification: 0x37c7 (14279)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51c [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 56400, Dst Port: 53
Source Port: 56400
Destination Port: 53
Length: 51
Checksum: 0xf682 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
Domain Name System (query)
Transaction ID: 0xe32a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
e9566.dsrb.akamaiedge.net: type A, class IN
Name: e9566.dsrb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 9]
No. Time Source Destination Protocol Length Info
8 2018-10-17 16:36:31.975845 10.173.88.157 218.30.19.40 DNS 93 Standard query 0xe32a
A e9566.dsrb.akamaiedge.net
Frame 8: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.975845000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.975845000 seconds
[Time delta from previous captured frame: 0.027840000 seconds]
[Time delta from previous displayed frame: 0.027840000 seconds]
[Time since reference or first frame: 1.732378000 seconds]
Frame Number: 8

Frame Length: 93 bytes (744 bits)
Capture Length: 93 bytes (744 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 73

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 71
Identification: 0x626d (25197)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a8 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 56400, Dst Port: 53
Source Port: 56400
Destination Port: 53
Length: 51
Checksum: 0x43b5 [unverified]
[Checksum Status: Unverified]
[Stream index: 4]

Domain Name System (query)
Transaction ID: 0xe32a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0.. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
e9566.dsrb.akamaiedge.net: type A, class IN
Name: e9566.dsrb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 16]

No.	Time	Source	Destination	Protocol	Length	Info
9	2018-10-17 16:36:31.996641	202.117.112.3	10.173.88.157	DNS	330	Standard query response
0xe32a	A e9566.dsrb.akamaiedge.net	A 184.26.244.21	NS f.gtld-servers.net	NS a.gtld-servers.net	NS j.gtld-servers.net	NS
c.gtld-servers.net	NS e.gtld-servers.net	NS h.gtld-servers.net	NS m.gtld-servers.net	NS b.gtld-servers.net	NS g.gtld-servers.net	NS l.gtld-servers.net
i.gtld-servers.net	NS d.gtld-servers.net	NS k.gtld-servers.net				

Frame 9: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.996641000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.996641000 seconds
[Time delta from previous captured frame: 0.020796000 seconds]
[Time delta from previous displayed frame: 0.020796000 seconds]
[Time since reference or first frame: 1.753174000 seconds]
Frame Number: 9
Frame Length: 330 bytes (2640 bits)
Capture Length: 330 bytes (2640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 310
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 308
Identification: 0x51f2 (20978)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e04 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 56400
Source Port: 53
Destination Port: 56400
Length: 288
Checksum: 0x5d5e [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
Domain Name System (response)
 Transaction ID: 0xe32a
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0... = Z: reserved (0)
 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
 0.... = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

e9566.dscb.akamaiedge.net: type A, class IN
Name: e9566.dscb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

e9566.dscb.akamaiedge.net: type A, class IN, addr 184.26.244.21
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 184.26.244.21

Authoritative nameservers

net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 17

Name Server: f.gtld-servers.net

net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: a.gtld-servers.net

net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: j.gtld-servers.net

net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: c.gtld-servers.net

net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: e.gtld-servers.net

net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: h.gtld-servers.net

net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: m.gtld-servers.net

net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 169191

Data length: 4

Name Server: b.gtld-servers.net

net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: g.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: l.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: i.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: d.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: k.gtld-servers.net
[Request In: 7]
[Time: 0.048636000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
10	2018-10-17 16:36:31.996643	202.117.112.3	10.173.88.157	DNS	389	Standard query response

0xbfb8 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.26.244.21 NS i.gtld-servers.net NS e.gtld-servers.net NS h.gtld-servers.net NS g.gtld-servers.net NS b.gtld-servers.net NS l.gtld-servers.net NS c.gtld-servers.net NS a.gtld-servers.net NS f.gtld-servers.net NS m.gtld-servers.net NS j.gtld-servers.net NS k.gtld-servers.net NS d.gtld-servers.net

Frame 10: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.996643000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.996643000 seconds
[Time delta from previous captured frame: 0.000002000 seconds]
[Time delta from previous displayed frame: 0.000002000 seconds]
[Time since reference or first frame: 1.753176000 seconds]
Frame Number: 10
Frame Length: 389 bytes (3112 bits)
Capture Length: 389 bytes (3112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 369
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 367
Identification: 0x51f3 (20979)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dc8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55223
Source Port: 53
Destination Port: 55223
Length: 347
Checksum: 0x1f04 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Domain Name System (response)
Transaction ID: 0xbfb8
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1.... = Recursion available: Server can do recursive queries
 0. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0. = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 13
Additional RRs: 0
Queries
 www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
 www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 Name: www.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1486
 Data length: 25
 CNAME: www.mit.edu.edgekey.net
 www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dsrb.akamaiedge.net
 Name: www.mit.edu.edgekey.net
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 24
 CNAME: e9566.dsrb.akamaiedge.net
 e9566.dsrb.akamaiedge.net: type A, class IN, addr 184.26.244.21
 Name: e9566.dsrb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 4
 Address: 184.26.244.21
Authoritative nameservers
 net: type NS, class IN, ns i.gtld-servers.net
 Name: net
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169191

Data length: 17
Name Server: i.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: h.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: g.gtld-servers.net
net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: b.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: l.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: c.gtld-servers.net
net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: a.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: f.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: m.gtld-servers.net
net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: j.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191

Data length: 4
Name Server: k.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: d.gtld-servers.net
[Request In: 3]
[Time: 0.160291000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
11	2018-10-17 16:36:31.998541	10.173.88.157	202.117.112.3	DNS	93	Standard query 0xd1bd

AAAA e9566.dscb.akamaiedge.net
Frame 11: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:31.998541000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765391.998541000 seconds
[Time delta from previous captured frame: 0.001898000 seconds]
[Time delta from previous displayed frame: 0.001898000 seconds]
[Time since reference or first frame: 1.755074000 seconds]
Frame Number: 11
Frame Length: 93 bytes (744 bits)
Capture Length: 93 bytes (744 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 73
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 71
Identification: 0x37c8 (14280)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51b [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 52894, Dst Port: 53
Source Port: 52894
Destination Port: 53
Length: 51
Checksum: 0xfaa1 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
Domain Name System (query)

Transaction ID: 0xd1bd
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
e9566.dscb.akamaiedge.net: type AAAA, class IN
 Name: e9566.dscb.akamaiedge.net
 [Name Length: 25]
 [Label Count: 4]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 18]
No. Time Source Destination Protocol Length Info
15 2018-10-17 16:36:32.025156 10.173.88.157 218.30.19.40 DNS 93 Standard query 0xd1bd
AAAA e9566.dscb.akamaiedge.net
Frame 15: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:32.025156000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765392.025156000 seconds
[Time delta from previous captured frame: 0.025543000 seconds]
[Time delta from previous displayed frame: 0.026615000 seconds]
[Time since reference or first frame: 1.781689000 seconds]
Frame Number: 15
Frame Length: 93 bytes (744 bits)
Capture Length: 93 bytes (744 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 73
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 71
Identification: 0x626e (25198)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
.... 00.. = More fragments: Not set
.... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157

Destination: 218.30.19.40
User Datagram Protocol, Src Port: 52894, Dst Port: 53
Source Port: 52894
Destination Port: 53
Length: 51
Checksum: 0x47d4 [unverified]
[Checksum Status: Unverified]
[Stream index: 6]
Domain Name System (query)
Transaction ID: 0xd1bd
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
e9566.dsrb.akamaiedge.net: type AAAA, class IN
 Name: e9566.dsrb.akamaiedge.net
 [Name Length: 25]
 [Label Count: 4]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 28]
No. Time Source Destination Protocol Length Info
16 2018-10-17 16:36:32.035178 218.30.19.40 10.173.88.157 DNS 109 Standard query response
0xe32a A e9566.dsrb.akamaiedge.net A 23.2.132.180
Frame 16: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:32.035178000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765392.035178000 seconds
[Time delta from previous captured frame: 0.010022000 seconds]
[Time delta from previous displayed frame: 0.010022000 seconds]
[Time since reference or first frame: 1.791711000 seconds]
Frame Number: 16
Frame Length: 109 bytes (872 bits)
Capture Length: 109 bytes (872 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 89
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 87
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment

0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf105 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 56400
Source Port: 53
Destination Port: 56400
Length: 67
Checksum: 0xcdb6 [unverified]
[Checksum Status: Unverified]
[Stream index: 4]

Domain Name System (response)
Transaction ID: 0xe32a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries
e9566.dsrb.akamaiedge.net: type A, class IN
Name: e9566.dsrb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
e9566.dsrb.akamaiedge.net: type A, class IN, addr 23.2.132.180
Name: e9566.dsrb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 23.2.132.180
[Request In: 8]
[Time: 0.059333000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
18	2018-10-17 16:36:32.059368	202.117.112.3	10.173.88.157	DNS	370	Standard query response

0xd1bd AAAA e9566.dsrb.akamaiedge.net AAAA 2600:1404:a:3a2::255e AAAA 2600:1404:a:393::255e NS j.gtld-servers.net NS h.gtld-servers.net NS g.gtld-servers.net NS k.gtld-servers.net NS i.gtld-servers.net NS a.gtld-servers.net NS b.gtld-servers.net NS c.gtld-servers.net NS f.gtld-servers.net NS e.gtld-servers.net NS m.gtld-servers.net NS d.gtld-servers.net NS l.gtld-servers.net

Frame 18: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:32.059368000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765392.059368000 seconds
[Time delta from previous captured frame: 0.008835000 seconds]
[Time delta from previous displayed frame: 0.024190000 seconds]
[Time since reference or first frame: 1.815901000 seconds]
Frame Number: 18
Frame Length: 370 bytes (2960 bits)
Capture Length: 370 bytes (2960 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 350

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 348
Identification: 0x51f4 (20980)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dda [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 52894
Source Port: 53
Destination Port: 52894
Length: 328
Checksum: 0xf174 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
Domain Name System (response)
Transaction ID: 0xd1bd
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 13
Additional RRs: 0
Queries
e9566.dsrb.akamaiedge.net: type AAAA, class IN
Name: e9566.dsrb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
e9566.dsrb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:a:3a2::255e
Name: e9566.dsrb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2600:1404:a:3a2::255e
e9566.dsrb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:a:393::255e
Name: e9566.dsrb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2600:1404:a:393::255e

Authoritative nameservers

net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 17
Name Server: j.gtld-servers.net

net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: h.gtld-servers.net

net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: g.gtld-servers.net

net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: k.gtld-servers.net

net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: i.gtld-servers.net

net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: a.gtld-servers.net

net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: b.gtld-servers.net

net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: c.gtld-servers.net

net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: f.gtld-servers.net

net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: e.gtld-servers.net

net: type NS, class IN, ns m.gtld-servers.net
Name: net

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: m.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: d.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169191
Data length: 4
Name Server: l.gtld-servers.net
[Request In: 11]
[Time: 0.060827000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
28	2018-10-17 16:36:32.097345	218.30.19.40	10.173.88.157	DNS	149	Standard query response 0xd1bd AAAA e9566.dscb.akamaiedge.net AAAA 2600:1404:a:393::255e AAAA 2600:1404:a:3a2::255e

Frame 28: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:32.097345000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765392.097345000 seconds
[Time delta from previous captured frame: 0.013755000 seconds]
[Time delta from previous displayed frame: 0.037977000 seconds]
[Time since reference or first frame: 1.853878000 seconds]
Frame Number: 28
Frame Length: 149 bytes (1192 bits)
Capture Length: 149 bytes (1192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 129
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 127
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0dd [validation disabled]
[Header checksum status: Unverified]

Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 52894
Source Port: 53
Destination Port: 52894
Length: 107
Checksum: 0xed98 [unverified]
[Checksum Status: Unverified]
[Stream index: 6]
Domain Name System (response)
Transaction ID: 0xd1bd
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
e9566.dsrb.akamaiedge.net: type AAAA, class IN
Name: e9566.dsrb.akamaiedge.net
[Name Length: 25]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
e9566.dsrb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:a:393::255e
Name: e9566.dsrb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2600:1404:a:393::255e
e9566.dsrb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:a:3a2::255e
Name: e9566.dsrb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2600:1404:a:3a2::255e
[Request In: 15]
[Time: 0.072189000 seconds]
No. Time Source Destination Protocol Length Info
905 2018-10-17 16:36:33.422747 10.173.88.157 202.117.112.3 DNS 80 Standard query 0x7f06
A news.mit.edu
Frame 905: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.422747000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.422747000 seconds
[Time delta from previous captured frame: 0.021183000 seconds]
[Time delta from previous displayed frame: 1.325402000 seconds]
[Time since reference or first frame: 3.179280000 seconds]
Frame Number: 905
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 60

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 58
Identification: 0x37c9 (14281)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa527 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 56283, Dst Port: 53
Source Port: 56283
Destination Port: 53
Length: 38
Checksum: 0x6d0a [unverified]
[Checksum Status: Unverified]
[Stream index: 7]

Domain Name System (query)
Transaction ID: 0x7f06
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
news.mit.edu: type A, class IN
Name: news.mit.edu
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 954]

No.	Time	Source	Destination	Protocol	Length	Info
906	2018-10-17 16:36:33.423863	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xabf1

A eapsweb.mit.edu
Frame 906: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.423863000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.423863000 seconds
[Time delta from previous captured frame: 0.001116000 seconds]
[Time delta from previous displayed frame: 0.001116000 seconds]
[Time since reference or first frame: 3.180396000 seconds]
Frame Number: 906
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 61
Identification: 0x37ca (14282)
Flags: 0x0000
0.... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa523 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 58791, Dst Port: 53
Source Port: 58791
Destination Port: 53
Length: 41
Checksum: 0xb69e [unverified]
[Checksum Status: Unverified]
[Stream index: 8]

Domain Name System (query)
Transaction ID: 0xabf1
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
eapsweb.mit.edu: type A, class IN
Name: eapsweb.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 918]

No.	Time	Source	Destination	Protocol	Length	Info
907	2018-10-17 16:36:33.425347	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xafb3

A twitter.com
Frame 907: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.425347000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.425347000 seconds
[Time delta from previous captured frame: 0.001484000 seconds]
[Time delta from previous displayed frame: 0.001484000 seconds]
[Time since reference or first frame: 3.181880000 seconds]
Frame Number: 907
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37cb (14283)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa526 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 62971, Dst Port: 53
Source Port: 62971
Destination Port: 53
Length: 37
Checksum: 0xed66 [unverified]
[Checksum Status: Unverified]
[Stream index: 9]
Domain Name System (query)
Transaction ID: 0xafb3
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
twitter.com: type A, class IN
Name: twitter.com
[Name Length: 11]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 908]

No.	Time	Source	Destination	Protocol	Length	Info										
908	2018-10-17 16:36:33.428628	202.117.112.3	10.173.88.157	DNS	319	Standard query response										
0xafb3	A	twitter.com	31.13.66.23	NS g.gtld-servers.net	NS i.gtld-servers.net	NS m.gtld-servers.net	NS k.gtld-servers.net	NS e.gtld-servers.net	NS l.gtld-servers.net	NS a.gtld-servers.net	NS b.gtld-servers.net	NS j.gtld-servers.net	NS h.gtld-servers.net	NS d.gtld-servers.net	NS c.gtld-servers.net	NS f.gtld-servers.net
Frame 908: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits) on interface 0																
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})																
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}																
Encapsulation type: Ethernet (1)																
Arrival Time: Oct 17, 2018 16:36:33.428628000 中国标准时间																
[Time shift for this packet: 0.000000000 seconds]																
Epoch Time: 1539765393.428628000 seconds																
[Time delta from previous captured frame: 0.003281000 seconds]																
[Time delta from previous displayed frame: 0.003281000 seconds]																
[Time since reference or first frame: 3.185161000 seconds]																
Frame Number: 908																
Frame Length: 319 bytes (2552 bits)																
Capture Length: 319 bytes (2552 bits)																
[Frame is marked: False]																
[Frame is ignored: False]																
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]																
[Coloring Rule Name: UDP]																
[Coloring Rule String: udp]																
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)																
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)																
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)																
.... .0. = LG bit: Globally unique address (factory default)																
.... .0. = IG bit: Individual address (unicast)																
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)																
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)																
.... .0. = LG bit: Globally unique address (factory default)																
.... .0. = IG bit: Individual address (unicast)																
Type: PPPoE Session (0x8864)																
PPP-over-Ethernet Session																
0001 = Version: 1																
.... 0001 = Type: 1																
Code: Session Data (0x00)																
Session ID: 0x629d																
Payload Length: 299																
Point-to-Point Protocol																
Protocol: Internet Protocol version 4 (0x0021)																
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157																
0100 = Version: 4																
.... 0101 = Header Length: 20 bytes (5)																
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)																
0000 00.. = Differentiated Services Codepoint: Default (0)																
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)																
Total Length: 297																
Identification: 0x51f5 (20981)																
Flags: 0x0000																
0.... = Reserved bit: Not set																
.0.... = Don't fragment: Not set																
..0.... = More fragments: Not set																
...0 0000 0000 0000 = Fragment offset: 0																
Time to live: 60																
Protocol: UDP (17)																
Header checksum: 0x8e0c [validation disabled]																
[Header checksum status: Unverified]																
Source: 202.117.112.3																
Destination: 10.173.88.157																
User Datagram Protocol, Src Port: 53, Dst Port: 62971																
Source Port: 53																
Destination Port: 62971																
Length: 277																
Checksum: 0xeb0a [unverified]																
[Checksum Status: Unverified]																
[Stream index: 9]																
Domain Name System (response)																
Transaction ID: 0xafb3																
Flags: 0x8180 Standard query response, No error																
1.... = Response: Message is a response																
.000 0.... = Opcode: Standard query (0)																
.... .0. = Authoritative: Server is not an authority for domain																
.... ..0. = Truncated: Message is not truncated																
.... ...1 = Recursion desired: Do query recursively																
.... 1.... = Recursion available: Server can do recursive queries																
....0.... = Z: reserved (0)																

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

twitter.com: type A, class IN
Name: twitter.com
[Name Length: 11]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

twitter.com: type A, class IN, addr 31.13.66.23
Name: twitter.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 167
Data length: 4
Address: 31.13.66.23

Authoritative nameservers

com: type NS, class IN, ns g.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 20
Name Server: g.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: i.gtld-servers.net
com: type NS, class IN, ns m.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: m.gtld-servers.net
com: type NS, class IN, ns k.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: k.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: e.gtld-servers.net
com: type NS, class IN, ns l.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: l.gtld-servers.net
com: type NS, class IN, ns a.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: a.gtld-servers.net

com: type NS, class IN, ns b.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182

Data length: 4
Name Server: b.gtld-servers.net
com: type NS, class IN, ns j.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: j.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: h.gtld-servers.net
com: type NS, class IN, ns d.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: d.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: c.gtld-servers.net
com: type NS, class IN, ns f.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: f.gtld-servers.net
[Request In: 907]
[Time: 0.003281000 seconds]
No. Time Source Destination Protocol Length Info
909 2018-10-17 16:36:33.429714 10.173.88.157 202.117.112.3 DNS 79 Standard query 0x8893
A twitter.com
Frame 909: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.429714000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.429714000 seconds
[Time delta from previous captured frame: 0.001086000 seconds]
[Time delta from previous displayed frame: 0.001086000 seconds]
[Time since reference or first frame: 3.186247000 seconds]
Frame Number: 909
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37cc (14284)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa525 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 60823, Dst Port: 53
Source Port: 60823
Destination Port: 53
Length: 37
Checksum: 0x1ceb [unverified]
[Checksum Status: Unverified]
[Stream index: 10]
Domain Name System (query)
Transaction ID: 0x8893
Flags: 0x0100 Standard query
 0.... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0... = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 twitter.com: type A, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 910]
No. Time Source Destination Protocol Length Info
910 2018-10-17 16:36:33.430458 202.117.112.3 10.173.88.157 DNS 319 Standard query response
0x8893 A twitter.com A 31.13.66.23 NS k.gtld-servers.net NS g.gtld-servers.net NS h.gtld-servers.net NS d.gtld-servers.net
NS m.gtld-servers.net NS i.gtld-servers.net NS j.gtld-servers.net NS c.gtld-servers.net NS l.gtld-servers.net NS b.gtld-
servers.net NS f.gtld-servers.net NS a.gtld-servers.net NS e.gtld-servers.net
Frame 910: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.430458000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.430458000 seconds
[Time delta from previous captured frame: 0.000744000 seconds]
[Time delta from previous displayed frame: 0.000744000 seconds]
[Time since reference or first frame: 3.186991000 seconds]
Frame Number: 910
Frame Length: 319 bytes (2552 bits)
Capture Length: 319 bytes (2552 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 299

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 297

Identification: 0x51f6 (20982)

Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8e0b [validation disabled]
[Header checksum status: Unverified]

Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 60823
Source Port: 53
Destination Port: 60823
Length: 277
Checksum: 0x1b6f [unverified]
[Checksum Status: Unverified]
[Stream index: 10]

Domain Name System (response)
Transaction ID: 0x8893
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
twitter.com: type A, class IN
Name: twitter.com
[Name Length: 11]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
twitter.com: type A, class IN, addr 31.13.66.23
Name: twitter.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 167
Data length: 4
Address: 31.13.66.23

Authoritative nameservers
com: type NS, class IN, ns k.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 20

Name Server: k.gtld-servers.net
com: type NS, class IN, ns g.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: g.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: h.gtld-servers.net
com: type NS, class IN, ns d.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: d.gtld-servers.net
com: type NS, class IN, ns m.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: m.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: i.gtld-servers.net
com: type NS, class IN, ns j.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: j.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: c.gtld-servers.net
com: type NS, class IN, ns l.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: l.gtld-servers.net
com: type NS, class IN, ns b.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: b.gtld-servers.net
com: type NS, class IN, ns f.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: f.gtld-servers.net
com: type NS, class IN, ns a.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4

Name Server: a.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: e.gtld-servers.net
[Request In: 909]
[Time: 0.000744000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
911	2018-10-17 16:36:33.431430	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xffe8

AAAA twitter.com
Frame 911: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.431430000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.431430000 seconds
[Time delta from previous captured frame: 0.000972000 seconds]
[Time delta from previous displayed frame: 0.000972000 seconds]
[Time since reference or first frame: 3.187963000 seconds]
Frame Number: 911
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37cd (14285)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa524 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 61277, Dst Port: 53
Source Port: 61277
Destination Port: 53
Length: 37
Checksum: 0x88cf [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
Domain Name System (query)
Transaction ID: 0xffe8

Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 twitter.com: type AAAA, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1522]

No.	Time	Source	Destination	Protocol	Length	Info
912	2018-10-17 16:36:33.444493	10.173.88.157	218.30.19.40	DNS	80	Standard query 0x7f06

A news.mit.edu
Frame 912: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.444493000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.444493000 seconds
[Time delta from previous captured frame: 0.013063000 seconds]
[Time delta from previous displayed frame: 0.013063000 seconds]
[Time since reference or first frame: 3.201026000 seconds]
Frame Number: 912
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 60
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 58
Identification: 0x6270 (25200)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7b2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 56283, Dst Port: 53
Source Port: 56283
Destination Port: 53
Length: 38
Checksum: 0xba3c [unverified]
[Checksum Status: Unverified]
[Stream index: 12]
Domain Name System (query)
Transaction ID: 0x7f06
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
news.mit.edu: type A, class IN
 Name: news.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 934]
No. Time Source Destination Protocol Length Info
913 2018-10-17 16:36:33.444524 10.173.88.157 218.30.19.40 DNS 83 Standard query 0xabf1
A eapsweb.mit.edu
Frame 913: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.444524000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.444524000 seconds
[Time delta from previous captured frame: 0.000031000 seconds]
[Time delta from previous displayed frame: 0.000031000 seconds]
[Time since reference or first frame: 3.201057000 seconds]
Frame Number: 913
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x626f (25199)
Flags: 0x0000
0... = Reserved bit: Not set

.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7b0 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 58791, Dst Port: 53
Source Port: 58791
Destination Port: 53
Length: 41
Checksum: 0x03d1 [unverified]
[Checksum Status: Unverified]
[Stream index: 13]

Domain Name System (query)
Transaction ID: 0xabf1
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
.... 0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 eapsweb.mit.edu: type A, class IN
 Name: eapsweb.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 922]

No.	Time	Source	Destination	Protocol	Length	Info
914	2018-10-17 16:36:33.452362	10.173.88.157	202.117.112.3	DNS	117	Standard query 0x5f48

A znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com
Frame 914: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:33.452362000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765393.452362000 seconds
 [Time delta from previous captured frame: 0.007838000 seconds]
 [Time delta from previous displayed frame: 0.007838000 seconds]
 [Time since reference or first frame: 3.208895000 seconds]
 Frame Number: 914
 Frame Length: 117 bytes (936 bits)
 Capture Length: 117 bytes (936 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

 Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

 Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 97

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..0 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 95
Identification: 0x37ce (14286)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fd [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 56114, Dst Port: 53
Source Port: 56114
Destination Port: 53
Length: 75
Checksum: 0x52ac [unverified]
[Checksum Status: Unverified]
[Stream index: 14]
Domain Name System (query)
Transaction ID: 0x5f48
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0... = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com: type A, class IN
Name: znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com
[Name Length: 49]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 915]
No. Time Source Destination Protocol Length Info
915 2018-10-17 16:36:33.454411 202.117.112.3 10.173.88.157 DNS 434 Standard query response
0x5f48 A znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com CNAME cloud.qualtrics.com.edgekey.net CNAME
e3672.ksd.akamaiedge.net A 23.11.246.32 NS b.gtld-servers.net NS g.gtld-servers.net NS k.gtld-servers.net NS d.gtld-
servers.net NS j.gtld-servers.net NS f.gtld-servers.net NS a.gtld-servers.net NS l.gtld-servers.net NS h.gtld-servers.net NS
i.gtld-servers.net NS m.gtld-servers.net NS e.gtld-servers.net NS c.gtld-servers.net
Frame 915: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.454411000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.454411000 seconds
[Time delta from previous captured frame: 0.002049000 seconds]
[Time delta from previous displayed frame: 0.002049000 seconds]
[Time since reference or first frame: 3.210944000 seconds]
Frame Number: 915
Frame Length: 434 bytes (3472 bits)
Capture Length: 434 bytes (3472 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 414

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 412
Identification: 0x51f7 (20983)
Flags: 0x0000

0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8d97 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 56114

Source Port: 53
Destination Port: 56114
Length: 392
Checksum: 0x7901 [unverified]
[Checksum Status: Unverified]
[Stream index: 14]

Domain Name System (response)

Transaction ID: 0x5f48

Flags: 0x8180 Standard query response, No error

1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 3
Authority RRs: 13
Additional RRs: 0

Queries

znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com: type A, class IN
 Name: znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com
 [Name Length: 49]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com: type CNAME, class IN, cname cloud.qualtrics.com.edgekey.net
 Name: znbsgdeu4idqsr8db-mit.siteintercept.qualtrics.com
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 3290
 Data length: 33
 CNAME: cloud.qualtrics.com.edgekey.net

cloud.qualtrics.com.edgekey.net: type CNAME, class IN, cname e3672.ksd.akamaiedge.net
 Name: cloud.qualtrics.com.edgekey.net
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 191
 Data length: 23
 CNAME: e3672.ksd.akamaiedge.net

e3672.ksd.akamaiedge.net: type A, class IN, addr 23.11.246.32

Name: e3672.ksd.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 191
Data length: 4
Address: 23.11.246.32

Authoritative nameservers

net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 17
Name Server: b.gtld-servers.net

net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: g.gtld-servers.net

net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: k.gtld-servers.net

net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: d.gtld-servers.net

net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: j.gtld-servers.net

net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: f.gtld-servers.net

net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: a.gtld-servers.net

net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: l.gtld-servers.net

net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: h.gtld-servers.net

net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: i.gtld-servers.net

```
net: type NS, class IN, ns m.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169189
  Data length: 4
  Name Server: m.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169189
  Data length: 4
  Name Server: e.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169189
  Data length: 4
  Name Server: c.gtld-servers.net
[Request In: 914]
[Time: 0.002049000 seconds]
No.  Time                               Source                Destination           Protocol Length Info
 917 2018-10-17 16:36:33.464679    10.173.88.157      218.30.19.40        DNS      79      Standard query 0xffe8
AAAA twitter.com
Frame 917: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
  Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.464679000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.464679000 seconds
[Time delta from previous captured frame: 0.004142000 seconds]
[Time delta from previous displayed frame: 0.010268000 seconds]
[Time since reference or first frame: 3.221212000 seconds]
Frame Number: 917
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
  Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
  .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
  .... ..0. .... .... .... = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
  Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
  .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
  .... ..0. .... .... .... = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
  0001 .... = Version: 1
  .... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
  Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x6271 (25201)
Flags: 0x0000
  0... .... .... .... = Reserved bit: Not set
  .0... .... .... .... = Don't fragment: Not set
  ..0. .... .... .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
```

Header checksum: 0xc7b2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 61277, Dst Port: 53
Source Port: 61277
Destination Port: 53
Length: 37
Checksum: 0xd601 [unverified]
[Checksum Status: Unverified]
[Stream index: 15]
Domain Name System (query)
Transaction ID: 0xffe8
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 twitter.com: type AAAA, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 946]
No. Time Source Destination Protocol Length Info
918 2018-10-17 16:36:33.475769 202.117.112.3 10.173.88.157 DNS 322 Standard query response
0xabf1 A eapsweb.mit.edu A 18.83.3.132 NS b.edu-servers.net NS e.edu-servers.net NS i.edu-servers.net NS h.edu-servers.net
NS a.edu-servers.net NS j.edu-servers.net NS l.edu-servers.net NS c.edu-servers.net NS d.edu-servers.net NS f.edu-
servers.net NS m.edu-servers.net NS k.edu-servers.net g.edu-servers.net
Frame 918: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.475769000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.475769000 seconds
[Time delta from previous captured frame: 0.011090000 seconds]
[Time delta from previous displayed frame: 0.011090000 seconds]
[Time since reference or first frame: 3.232302000 seconds]
Frame Number: 918
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 300
Identification: 0x51f8 (20984)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e06 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 58791
Source Port: 53
Destination Port: 58791
Length: 280
Checksum: 0xcde9 [unverified]
[Checksum Status: Unverified]
[Stream index: 8]

Domain Name System (response)
Transaction ID: 0xabf1
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0. = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1... = Recursion available: Server can do recursive queries
.0... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0 = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
eapsweb.mit.edu: type A, class IN
Name: eapsweb.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
eapsweb.mit.edu: type A, class IN, addr 18.83.3.132
Name: eapsweb.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.83.3.132

Authoritative nameservers
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 19
Name Server: b.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: i.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net

Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: h.edu-servers.net
 edu: type NS, class IN, ns a.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: a.edu-servers.net
 edu: type NS, class IN, ns j.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: j.edu-servers.net
 edu: type NS, class IN, ns l.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: l.edu-servers.net
 edu: type NS, class IN, ns c.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: c.edu-servers.net
 edu: type NS, class IN, ns d.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: d.edu-servers.net
 edu: type NS, class IN, ns f.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: f.edu-servers.net
 edu: type NS, class IN, ns m.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: m.edu-servers.net
 edu: type NS, class IN, ns k.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: k.edu-servers.net
 edu: type NS, class IN, ns g.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: g.edu-servers.net

[Request In: 906]

[Time: 0.051906000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
919	2018-10-17 16:36:33.476620	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x7dcf

A eapsweb.mit.edu

Frame 919: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.476620000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.476620000 seconds
[Time delta from previous captured frame: 0.000851000 seconds]
[Time delta from previous displayed frame: 0.000851000 seconds]
[Time since reference or first frame: 3.233153000 seconds]
Frame Number: 919
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37cf (14287)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51e [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 55957, Dst Port: 53
Source Port: 55957
Destination Port: 53
Length: 41
Checksum: 0xefd2 [unverified]
[Checksum Status: Unverified]
[Stream index: 16]
Domain Name System (query)
Transaction ID: 0x7dcf
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
eapsweb.mit.edu: type A, class IN
Name: eapsweb.mit.edu
[Name Length: 15]
[Label Count: 3]

Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 920]
No. Time Source Destination Protocol Length Info
920 2018-10-17 16:36:33.477412 202.117.112.3 10.173.88.157 DNS 322 Standard query response
0x7dcf A eapsweb.mit.edu A 18.83.3.132 NS a.edu-servers.net NS d.edu-servers.net NS k.edu-servers.net NS g.edu-servers.net
NS i.edu-servers.net NS m.edu-servers.net NS j.edu-servers.net NS l.edu-servers.net NS c.edu-servers.net NS b.edu-
servers.net NS h.edu-servers.net NS f.edu-servers.net NS e.edu-servers.net
Frame 920: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.477412000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.477412000 seconds
[Time delta from previous captured frame: 0.000792000 seconds]
[Time delta from previous displayed frame: 0.000792000 seconds]
[Time since reference or first frame: 3.233945000 seconds]
Frame Number: 920
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 300
Identification: 0x51f9 (20985)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e05 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55957
Source Port: 53
Destination Port: 55957
Length: 280
Checksum: 0x081d [unverified]
[Checksum Status: Unverified]
[Stream index: 16]
Domain Name System (response)
Transaction ID: 0x7dcf
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
. 0. = Authoritative: Server is not an authority for domain
. 0. = Truncated: Message is not truncated

.... 1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
.... 0... = Z: reserved (0)
.... ...0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... ...0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

eapsweb.mit.edu: type A, class IN
 Name: eapsweb.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

eapsweb.mit.edu: type A, class IN, addr 18.83.3.132
 Name: eapsweb.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.83.3.132

Authoritative nameservers

edu: type NS, class IN, ns a.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 19
 Name Server: a.edu-servers.net

edu: type NS, class IN, ns d.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: d.edu-servers.net

edu: type NS, class IN, ns k.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: k.edu-servers.net

edu: type NS, class IN, ns g.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: g.edu-servers.net

edu: type NS, class IN, ns i.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: i.edu-servers.net

edu: type NS, class IN, ns m.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: m.edu-servers.net

edu: type NS, class IN, ns j.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: j.edu-servers.net

edu: type NS, class IN, ns l.edu-servers.net
 Name: edu

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: c.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: h.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: e.edu-servers.net

[Request In: 919]
[Time: 0.000792000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
921	2018-10-17 16:36:33.478056	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xf7c3

AAAA eapsweb.mit.edu

Frame 921: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.478056000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.478056000 seconds
[Time delta from previous captured frame: 0.000644000 seconds]
[Time delta from previous displayed frame: 0.000644000 seconds]
[Time since reference or first frame: 3.234589000 seconds]
Frame Number: 921
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)

Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37d0 (14288)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51d [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 61737, Dst Port: 53
Source Port: 61737
Destination Port: 53
Length: 41
Checksum: 0x444a [unverified]
[Checksum Status: Unverified]
[Stream index: 17]
Domain Name System (query)
Transaction ID: 0xf7c3
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
eapsweb.mit.edu: type AAAA, class IN
Name: eapsweb.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 924]
No. Time Source Destination Protocol Length Info
922 2018-10-17 16:36:33.497661 218.30.19.40 10.173.88.157 DNS 99 Standard query response
0xabf1 A eapsweb.mit.edu A 18.83.3.132
Frame 922: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.497661000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.497661000 seconds
[Time delta from previous captured frame: 0.019605000 seconds]
[Time delta from previous displayed frame: 0.019605000 seconds]
[Time since reference or first frame: 3.254194000 seconds]
Frame Number: 922
Frame Length: 99 bytes (792 bits)
Capture Length: 99 bytes (792 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 79
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 77
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0.... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf10f [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 58791
Source Port: 53
Destination Port: 58791
Length: 57
Checksum: 0x9152 [unverified]
[Checksum Status: Unverified]
[Stream index: 13]
Domain Name System (response)
Transaction ID: 0xabf1
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
eapsweb.mit.edu: type A, class IN
Name: eapsweb.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
eapsweb.mit.edu: type A, class IN, addr 18.83.3.132
Name: eapsweb.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.83.3.132
[Request In: 913]
[Time: 0.053137000 seconds]
No. Time Source Destination Protocol Length Info
923 2018-10-17 16:36:33.505349 10.173.88.157 218.30.19.40 DNS 83 Standard query 0xf7c3
AAAA eapsweb.mit.edu
Frame 923: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.505349000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.505349000 seconds
[Time delta from previous captured frame: 0.007688000 seconds]
[Time delta from previous displayed frame: 0.007688000 seconds]
[Time since reference or first frame: 3.261882000 seconds]
Frame Number: 923
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x6272 (25202)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7ad [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 61737, Dst Port: 53
Source Port: 61737
Destination Port: 53
Length: 41
Checksum: 0x917c [unverified]
[Checksum Status: Unverified]
[Stream index: 18]
Domain Name System (query)
Transaction ID: 0xf7c3
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
....0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
eapsweb.mit.edu: type AAAA, class IN
Name: eapsweb.mit.edu

[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 925]

No.	Time	Source	Destination	Protocol	Length	Info
924	2018-10-17 16:36:33.527269	202.117.112.3	10.173.88.157	DNS	148	Standard query response

0xf7c3 AAAA eapsweb.mit.edu SOA use2.akam.net
Frame 924: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.527269000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.527269000 seconds
[Time delta from previous captured frame: 0.021920000 seconds]
[Time delta from previous displayed frame: 0.021920000 seconds]
[Time since reference or first frame: 3.283802000 seconds]
Frame Number: 924
Frame Length: 148 bytes (1184 bits)
Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 128
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 126
Identification: 0x51fa (20986)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8eb2 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61737
Source Port: 53
Destination Port: 61737
Length: 106
Checksum: 0x8a5a [unverified]
[Checksum Status: Unverified]
[Stream index: 17]
Domain Name System (response)
Transaction ID: 0xf7c3
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively
.... ...1.... = Recursion available: Server can do recursive queries
.... ...0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

eapsweb.mit.edu: type AAAA, class IN

Name: eapsweb.mit.edu

[Name Length: 15]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Authoritative nameservers

mit.edu: type SOA, class IN, mname use2.akam.net

Name: mit.edu

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 900

Data length: 53

Primary name server: use2.akam.net

Responsible authority's mailbox: network-request.mit.edu

Serial Number: 11252

Refresh Interval: 900 (15 minutes)

Retry Interval: 900 (15 minutes)

Expire limit: 3600000 (41 days, 16 hours)

Minimum TTL: 3600 (1 hour)

[Request In: 921]

[Time: 0.049213000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
925	2018-10-17 16:36:33.529014	218.30.19.40	10.173.88.157	DNS	148	Standard query response

0xf7c3 AAAA eapsweb.mit.edu use2.akam.net

Frame 925: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.529014000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.529014000 seconds

[Time delta from previous captured frame: 0.001745000 seconds]

[Time delta from previous displayed frame: 0.001745000 seconds]

[Time since reference or first frame: 3.285547000 seconds]

Frame Number: 925

Frame Length: 148 bytes (1184 bits)

Capture Length: 148 bytes (1184 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... ...0.... = LG bit: Globally unique address (factory default)

.... ...0.... = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ...0.... = LG bit: Globally unique address (factory default)

.... ...0.... = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 128

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 126
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0de [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61737
Source Port: 53
Destination Port: 61737
Length: 106
Checksum: 0xd78c [unverified]
[Checksum Status: Unverified]
[Stream index: 18]
Domain Name System (response)
Transaction ID: 0xf7c3
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0. = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
.0.... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0.... = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
 eapsweb.mit.edu: type AAAA, class IN
 Name: eapsweb.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
Authoritative nameservers
 mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 900
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)
 [Request In: 923]
 [Time: 0.023665000 seconds]
No. Time Source Destination Protocol Length Info
926 2018-10-17 16:36:33.531694 10.173.88.157 202.117.112.3 DNS 84 Standard query 0x14d4
A www.facebook.com
Frame 926: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.531694000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.531694000 seconds
[Time delta from previous captured frame: 0.002680000 seconds]
[Time delta from previous displayed frame: 0.002680000 seconds]
[Time since reference or first frame: 3.288227000 seconds]
Frame Number: 926
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)

[Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 64

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 62
 Identification: 0x37d1 (14289)
 Flags: 0x0000
 0.... = Reserved bit: Not set
 .0.... = Don't fragment: Not set
 ..0.... = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa51b [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.173.88.157
 Destination: 202.117.112.3

User Datagram Protocol, Src Port: 61815, Dst Port: 53
 Source Port: 61815
 Destination Port: 53
 Length: 42
 Checksum: 0x6556 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 19]

Domain Name System (query)
 Transaction ID: 0x14d4
 Flags: 0x0100 Standard query
 0.... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0.. = Z: reserved (0)
0 = Non-authenticated data: Unacceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.facebook.com: type A, class IN
 Name: www.facebook.com
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 927]

No.	Time	Source	Destination	Protocol	Length	Info
927	2018-10-17 16:36:33.532677	202.117.112.3	10.173.88.157	DNS	191	Standard query response
0x14d4	A www.facebook.com	A 67.228.235.93	NS a.ns.facebook.com	NS b.ns.facebook.com	AAAA 2a03:2880:ffff:c:face:b00c:0:35	
AAAA	2a03:2880:ffff:c:face:b00c:0:35					

Frame 927: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.532677000 中国标准时间
[Time shift for this packet: 0.00000000 seconds]
Epoch Time: 1539765393.532677000 seconds
[Time delta from previous captured frame: 0.000983000 seconds]
[Time delta from previous displayed frame: 0.000983000 seconds]
[Time since reference or first frame: 3.289210000 seconds]
Frame Number: 927
Frame Length: 191 bytes (1528 bits)
Capture Length: 191 bytes (1528 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0 = LG bit: Globally unique address (factory default)
.... 0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0 = LG bit: Globally unique address (factory default)
.... 0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 171
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 169
Identification: 0x51fb (20987)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e86 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61815
Source Port: 53
Destination Port: 61815
Length: 149
Checksum: 0x8c79 [unverified]
[Checksum Status: Unverified]
[Stream index: 19]
Domain Name System (response)
Transaction ID: 0x14d4
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0. = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
Queries

www.facebook.com: type A, class IN
Name: www.facebook.com
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

www.facebook.com: type A, class IN, addr 67.228.235.93
Name: www.facebook.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 10
Data length: 4
Address: 67.228.235.93

Authoritative nameservers

facebook.com: type NS, class IN, ns a.ns.facebook.com
Name: facebook.com

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171535
Data length: 7

Name Server: a.ns.facebook.com

facebook.com: type NS, class IN, ns b.ns.facebook.com
Name: facebook.com

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171535
Data length: 4

Name Server: b.ns.facebook.com

Additional records

a.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:ffff:c:face:b00c:0:35

Name: a.ns.facebook.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 61961
Data length: 16

AAAA Address: 2a03:2880:ffff:c:face:b00c:0:35

b.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:ffff:c:face:b00c:0:35

Name: b.ns.facebook.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 120961
Data length: 16

AAAA Address: 2a03:2880:ffff:c:face:b00c:0:35

[Request In: 926]

[Time: 0.000983000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
928	2018-10-17 16:36:33.536900	10.173.88.157	202.117.112.3	DNS	84	Standard query 0xf7ba

AAAA www.facebook.com

Frame 928: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.536900000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.536900000 seconds

[Time delta from previous captured frame: 0.004223000 seconds]

[Time delta from previous displayed frame: 0.004223000 seconds]

[Time since reference or first frame: 3.293433000 seconds]

Frame Number: 928

Frame Length: 84 bytes (672 bits)

Capture Length: 84 bytes (672 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37d2 (14290)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51a [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 62405, Dst Port: 53
Source Port: 62405
Destination Port: 53
Length: 42
Checksum: 0x8006 [unverified]
[Checksum Status: Unverified]
[Stream index: 20]
Domain Name System (query)
Transaction ID: 0xf7ba
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.facebook.com: type AAAA, class IN
Name: www.facebook.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 929]
No. Time Source Destination Protocol Length Info
929 2018-10-17 16:36:33.538271 202.117.112.3 10.173.88.157 DNS 203 Standard query response
0xf7ba AAAA www.facebook.com AAAA 2400:cb00:2048:1::6814:224e NS b.ns.facebook.com NS a.ns.facebook.com AAAA
2a03:2880:ffff:c:face:b00c:0:35 AAAA 2a03:2880:ffff:c:face:b00c:0:35
Frame 929: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.538271000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.538271000 seconds
[Time delta from previous captured frame: 0.001371000 seconds]
[Time delta from previous displayed frame: 0.001371000 seconds]
[Time since reference or first frame: 3.294804000 seconds]
Frame Number: 929
Frame Length: 203 bytes (1624 bits)
Capture Length: 203 bytes (1624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 183
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 181
Identification: 0x51fc (20988)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e79 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 62405
Source Port: 53
Destination Port: 62405
Length: 161
Checksum: 0x1960 [unverified]
[Checksum Status: Unverified]
[Stream index: 20]
Domain Name System (response)
Transaction ID: 0xf7ba
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 2
Additional RRs: 2
Queries
www.facebook.com: type AAAA, class IN
Name: www.facebook.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
www.facebook.com: type AAAA, class IN, addr 2400:cb00:2048:1::6814:224e
Name: www.facebook.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 41
Data length: 16
AAAA Address: 2400:cb00:2048:1::6814:224e
Authoritative nameservers

facebook.com: type NS, class IN, ns b.ns.facebook.com
Name: facebook.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171535
Data length: 7
Name Server: b.ns.facebook.com
facebook.com: type NS, class IN, ns a.ns.facebook.com
Name: facebook.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171535
Data length: 4
Name Server: a.ns.facebook.com
Additional records
a.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:ffff:c:face:b00c:0:35
Name: a.ns.facebook.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 61961
Data length: 16
AAAA Address: 2a03:2880:ffff:c:face:b00c:0:35
b.ns.facebook.com: type AAAA, class IN, addr 2a03:2880:ffff:c:face:b00c:0:35
Name: b.ns.facebook.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 120961
Data length: 16
AAAA Address: 2a03:2880:ffff:c:face:b00c:0:35
[Request In: 928]
[Time: 0.001371000 seconds]
No. Time Source Destination Protocol Length Info
930 2018-10-17 16:36:33.542057 10.173.88.157 202.117.112.3 DNS 82 Standard query 0xa6ac
A www.google.com
Frame 930: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.542057000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.542057000 seconds
[Time delta from previous captured frame: 0.003786000 seconds]
[Time delta from previous displayed frame: 0.003786000 seconds]
[Time since reference or first frame: 3.298590000 seconds]
Frame Number: 930
Frame Length: 82 bytes (656 bits)
Capture Length: 82 bytes (656 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 62
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 60

Identification: 0x37d3 (14291)
Flags: 0x0000
 0... = Reserved bit: Not set
 0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51b [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 56288, Dst Port: 53
Source Port: 56288
Destination Port: 53
Length: 40
Checksum: 0x5071 [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
Domain Name System (query)
Transaction ID: 0xa6ac
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0. = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 www.google.com: type A, class IN
 Name: www.google.com
 [Name Length: 14]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 931]
No. Time Source Destination Protocol Length Info
931 2018-10-17 16:36:33.543276 202.117.112.3 10.173.88.157 DNS 346 Standard query response
0xa6ac A www.google.com A 67.228.235.93 NS ns2.google.com NS ns3.google.com NS ns4.google.com NS ns1.google.com A
216.239.32.10 AAAA 2001:4860:4802:32::a A 216.239.34.10 AAAA 2001:4860:4802:34::a A 216.239.36.10 AAAA 2001:4860:4802:36::a
A 216.239.38.10 AAAA 2001:4860:4802:38::a
Frame 931: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.543276000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.543276000 seconds
[Time delta from previous captured frame: 0.001219000 seconds]
[Time delta from previous displayed frame: 0.001219000 seconds]
[Time since reference or first frame: 3.299809000 seconds]
Frame Number: 931
Frame Length: 346 bytes (2768 bits)
Capture Length: 346 bytes (2768 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0 = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)

Session ID: 0x629d
Payload Length: 326
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 324
Identification: 0x51fd (20989)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de9 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 56288
Source Port: 53
Destination Port: 56288
Length: 304
Checksum: 0x403d [unverified]
[Checksum Status: Unverified]
[Stream index: 21]
Domain Name System (response)
Transaction ID: 0xa6ac
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 4
Additional RRs: 8
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.google.com: type A, class IN, addr 67.228.235.93
Name: www.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 35
Data length: 4
Address: 67.228.235.93
Authoritative nameservers
google.com: type NS, class IN, ns ns2.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns2.google.com
google.com: type NS, class IN, ns ns3.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns3.google.com

```

google.com: type NS, class IN, ns ns4.google.com
  Name: google.com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 171639
  Data length: 6
  Name Server: ns4.google.com
google.com: type NS, class IN, ns ns1.google.com
  Name: google.com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 171639
  Data length: 6
  Name Server: ns1.google.com
Additional records
ns1.google.com: type A, class IN, addr 216.239.32.10
  Name: ns1.google.com
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 251764
  Data length: 4
  Address: 216.239.32.10
ns1.google.com: type AAAA, class IN, addr 2001:4860:4802:32::a
  Name: ns1.google.com
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 251767
  Data length: 16
  AAAA Address: 2001:4860:4802:32::a
ns2.google.com: type A, class IN, addr 216.239.34.10
  Name: ns2.google.com
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 251766
  Data length: 4
  Address: 216.239.34.10
ns2.google.com: type AAAA, class IN, addr 2001:4860:4802:34::a
  Name: ns2.google.com
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 278431
  Data length: 16
  AAAA Address: 2001:4860:4802:34::a
ns3.google.com: type A, class IN, addr 216.239.36.10
  Name: ns3.google.com
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 167608
  Data length: 4
  Address: 216.239.36.10
ns3.google.com: type AAAA, class IN, addr 2001:4860:4802:36::a
  Name: ns3.google.com
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 251770
  Data length: 16
  AAAA Address: 2001:4860:4802:36::a
ns4.google.com: type A, class IN, addr 216.239.38.10
  Name: ns4.google.com
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 251764
  Data length: 4
  Address: 216.239.38.10
ns4.google.com: type AAAA, class IN, addr 2001:4860:4802:38::a
  Name: ns4.google.com
  Type: AAAA (IPv6 Address) (28)
  Class: IN (0x0001)
  Time to live: 167755
  Data length: 16
  AAAA Address: 2001:4860:4802:38::a
[Request In: 930]
[Time: 0.001219000 seconds]

```

No.	Time	Source	Destination	Protocol	Length	Info
	932 2018-10-17 16:36:33.547069	10.173.88.157	202.117.112.3	DNS	82	Standard query 0xa2ca
AAAA www.google.com						
Frame 932: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0						

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.547069000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.547069000 seconds
[Time delta from previous captured frame: 0.003793000 seconds]
[Time delta from previous displayed frame: 0.003793000 seconds]
[Time since reference or first frame: 3.303602000 seconds]
Frame Number: 932
Frame Length: 82 bytes (656 bits)
Capture Length: 82 bytes (656 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x000)
Session ID: 0x629d
Payload Length: 62
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 60
Identification: 0x37d4 (14292)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa51a [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 58147, Dst Port: 53
Source Port: 58147
Destination Port: 53
Length: 40
Checksum: 0x4cf5 [unverified]
[Checksum Status: Unverified]
[Stream index: 22]
Domain Name System (query)
Transaction ID: 0xa2ca
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type AAAA, class IN
Name: www.google.com

[Name Length: 14]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 933]

No.	Time	Source	Destination	Protocol	Length	Info
933	2018-10-17 16:36:33.548161	202.117.112.3	10.173.88.157	DNS	358	Standard query response
0xa2ca	AAAA www.google.com AAAA 2400:cb00:2048:1::6814:224e NS ns2.google.com NS ns3.google.com NS ns4.google.com NS	ns1.google.com A 216.239.32.10 AAAA 2001:4860:4802:32::a A 216.239.34.10 AAAA 2001:4860:4802:34::a A 216.239.36.10 AAAA	2001:4860:4802:36::a A 216.239.38.10 AAAA 2001:4860:4802:38::a			

Frame 933: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.548161000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.548161000 seconds
[Time delta from previous captured frame: 0.001092000 seconds]
[Time delta from previous displayed frame: 0.001092000 seconds]
[Time since reference or first frame: 3.304694000 seconds]
Frame Number: 933
Frame Length: 358 bytes (2864 bits)
Capture Length: 358 bytes (2864 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 338
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 336
Identification: 0x51fe (20990)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8ddc [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 58147
Source Port: 53
Destination Port: 58147
Length: 316
Checksum: 0xd101 [unverified]
[Checksum Status: Unverified]
[Stream index: 22]
Domain Name System (response)
Transaction ID: 0xa2ca
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)

.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 4

Additional RRs: 8

Queries

www.google.com: type AAAA, class IN
 Name: www.google.com
 [Name Length: 14]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)

Answers

www.google.com: type AAAA, class IN, addr 2400:cb00:2048:1::6814:224e
 Name: www.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 217
 Data length: 16
 AAAA Address: 2400:cb00:2048:1::6814:224e

Authoritative nameservers

google.com: type NS, class IN, ns ns2.google.com
 Name: google.com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 171639
 Data length: 6
 Name Server: ns2.google.com
google.com: type NS, class IN, ns ns3.google.com
 Name: google.com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 171639
 Data length: 6
 Name Server: ns3.google.com
google.com: type NS, class IN, ns ns4.google.com
 Name: google.com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 171639
 Data length: 6
 Name Server: ns4.google.com
google.com: type NS, class IN, ns ns1.google.com
 Name: google.com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 171639
 Data length: 6
 Name Server: ns1.google.com

Additional records

ns1.google.com: type A, class IN, addr 216.239.32.10
 Name: ns1.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 251764
 Data length: 4
 Address: 216.239.32.10
ns1.google.com: type AAAA, class IN, addr 2001:4860:4802:32::a
 Name: ns1.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 251767
 Data length: 16
 AAAA Address: 2001:4860:4802:32::a
ns2.google.com: type A, class IN, addr 216.239.34.10
 Name: ns2.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 251766
 Data length: 4

Address: 216.239.34.10
ns2.google.com: type AAAA, class IN, addr 2001:4860:4802:34::a
Name: ns2.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 278431
Data length: 16
AAAA Address: 2001:4860:4802:34::a
ns3.google.com: type A, class IN, addr 216.239.36.10
Name: ns3.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 167608
Data length: 4
Address: 216.239.36.10
ns3.google.com: type AAAA, class IN, addr 2001:4860:4802:36::a
Name: ns3.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 251770
Data length: 16
AAAA Address: 2001:4860:4802:36::a
ns4.google.com: type A, class IN, addr 216.239.38.10
Name: ns4.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 251764
Data length: 4
Address: 216.239.38.10
ns4.google.com: type AAAA, class IN, addr 2001:4860:4802:38::a
Name: ns4.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 167755
Data length: 16
AAAA Address: 2001:4860:4802:38::a
[Request In: 932]
[Time: 0.001092000 seconds]
No. Time Source Destination Protocol Length Info
934 2018-10-17 16:36:33.549157 218.30.19.40 10.173.88.157 DNS 169 Standard query response
0x7f06 A news.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.2.132.180
Frame 934: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.549157000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.549157000 seconds
[Time delta from previous captured frame: 0.000996000 seconds]
[Time delta from previous displayed frame: 0.000996000 seconds]
[Time since reference or first frame: 3.305690000 seconds]
Frame Number: 934
Frame Length: 169 bytes (1352 bits)
Capture Length: 169 bytes (1352 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 149
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 147
 Identification: 0x0000 (0)
 Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 57
 Protocol: UDP (17)
 Header checksum: 0xf0c9 [validation disabled]
 [Header checksum status: Unverified]
 Source: 218.30.19.40
 Destination: 10.173.88.157
 User Datagram Protocol, Src Port: 53, Dst Port: 56283
 Source Port: 53
 Destination Port: 56283
 Length: 127
 Checksum: 0xf052 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 12]
 Domain Name System (response)
 Transaction ID: 0x7f06
 Flags: 0x8180 Standard query response, No error
 1... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0... = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0 = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
 Questions: 1
 Answer RRs: 3
 Authority RRs: 0
 Additional RRs: 0
 Queries
 news.mit.edu: type A, class IN
 Name: news.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 news.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 Name: news.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 25
 CNAME: www.mit.edu.edgekey.net
 www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dsrb.akamaiedge.net
 Name: www.mit.edu.edgekey.net
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 24
 CNAME: e9566.dsrb.akamaiedge.net
 e9566.dsrb.akamaiedge.net: type A, class IN, addr 23.2.132.180
 Name: e9566.dsrb.akamaiedge.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 298
 Data length: 4
 Address: 23.2.132.180
 [Request In: 912]
 [Time: 0.104664000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
935	2018-10-17 16:36:33.550940	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xdf41

A whereis.mit.edu

Frame 935: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.550940000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.550940000 seconds
[Time delta from previous captured frame: 0.001783000 seconds]
[Time delta from previous displayed frame: 0.001783000 seconds]
[Time since reference or first frame: 3.307473000 seconds]
Frame Number: 935
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37d5 (14293)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa518 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 50420, Dst Port: 53
Source Port: 50420
Destination Port: 53
Length: 41
Checksum: 0x99fb [unverified]
[Checksum Status: Unverified]
[Stream index: 23]
Domain Name System (query)
Transaction ID: 0xdf41
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0. = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 whereis.mit.edu: type A, class IN

Name: whereis.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 939]

No.	Time	Source	Destination	Protocol	Length	Info
936	2018-10-17 16:36:33.551130	10.173.88.157	202.117.112.3	DNS	84	Standard query 0x1494

A calendar.mit.edu

Frame 936: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.551130000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.551130000 seconds
[Time delta from previous captured frame: 0.000190000 seconds]
[Time delta from previous displayed frame: 0.000190000 seconds]
[Time since reference or first frame: 3.307663000 seconds]
Frame Number: 936
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37d6 (14294)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa516 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 57780, Dst Port: 53
Source Port: 57780
Destination Port: 53
Length: 42
Checksum: 0x08e2 [unverified]
[Checksum Status: Unverified]
[Stream index: 24]
Domain Name System (query)
Transaction ID: 0x1494
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 calendar.mit.edu: type A, class IN
 Name: calendar.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 1517]

No.	Time	Source	Destination	Protocol	Length	Info
937	2018-10-17 16:36:33.576285	10.173.88.157	218.30.19.40	DNS	83	Standard query 0xdf41

A whereis.mit.edu
Frame 937: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.576285000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.576285000 seconds
[Time delta from previous captured frame: 0.025155000 seconds]
[Time delta from previous displayed frame: 0.025155000 seconds]
[Time since reference or first frame: 3.332818000 seconds]
Frame Number: 937
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x6273 (25203)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7ac [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 50420, Dst Port: 53
 Source Port: 50420
 Destination Port: 53
 Length: 41

Checksum: 0xe72d [unverified]
[Checksum Status: Unverified]
[Stream index: 25]

Domain Name System (query)

Transaction ID: 0xdf41

Flags: 0x0100 Standard query

0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

 whereis.mit.edu: type A, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 943]

No.	Time	Source	Destination	Protocol	Length	Info
938	2018-10-17 16:36:33.577350	10.173.88.157	218.30.19.40	DNS	84	Standard query 0x1494

A calendar.mit.edu

Frame 938: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.577350000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.577350000 seconds
[Time delta from previous captured frame: 0.001065000 seconds]
[Time delta from previous displayed frame: 0.001065000 seconds]
[Time since reference or first frame: 3.333883000 seconds]

Frame Number: 938

Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 62

Identification: 0x6274 (25204)

Flags: 0x0000

0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64

Protocol: UDP (17)
Header checksum: 0xc7aa [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 57780, Dst Port: 53
Source Port: 57780
Destination Port: 53
Length: 42
Checksum: 0x5614 [unverified]
[Checksum Status: Unverified]
[Stream index: 26]
Domain Name System (query)
Transaction ID: 0x1494
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 calendar.mit.edu: type A, class IN
 Name: calendar.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1360]
No. Time Source Destination Protocol Length Info
939 2018-10-17 16:36:33.618213 202.117.112.3 10.173.88.157 DNS 322 Standard query response
0xdf41 A whereis.mit.edu A 18.7.76.12 NS e.edu-servers.net NS m.edu-servers.net NS c.edu-servers.net NS j.edu-servers.net NS i.edu-servers.net NS g.edu-servers.net NS k.edu-servers.net NS l.edu-servers.net NS d.edu-servers.net NS f.edu-servers.net NS h.edu-servers.net NS a.edu-servers.net NS b.edu-servers.net
Frame 939: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.618213000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.618213000 seconds
[Time delta from previous captured frame: 0.040863000 seconds]
[Time delta from previous displayed frame: 0.040863000 seconds]
[Time since reference or first frame: 3.374746000 seconds]
Frame Number: 939
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 300
Identification: 0x51ff (20991)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dff [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 50420
Source Port: 53
Destination Port: 50420
Length: 280
Checksum: 0x7201 [unverified]
[Checksum Status: Unverified]
[Stream index: 23]

Domain Name System (response)
Transaction ID: 0xdf41
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.0.... = Authoritative: Server is not an authority for domain
.0.... = Truncated: Message is not truncated
.1.... = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
.0.... = Z: reserved (0)
.0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
.0.... = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
whereis.mit.edu: type A, class IN
Name: whereis.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
whereis.mit.edu: type A, class IN, addr 18.7.76.12
Name: whereis.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.7.76.12

Authoritative nameservers
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 19
Name Server: e.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: m.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: c.edu-servers.net

```

edu: type NS, class IN, ns j.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: j.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: i.edu-servers.net
edu: type NS, class IN, ns g.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: g.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: k.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: l.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: d.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: f.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: h.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: a.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172720
  Data length: 4
  Name Server: b.edu-servers.net

```

[Request In: 935]
[Time: 0.067273000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
	940 2018-10-17 16:36:33.623197	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xabe2

A whereis.mit.edu

Frame 940: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.623197000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.623197000 seconds
[Time delta from previous captured frame: 0.004984000 seconds]
[Time delta from previous displayed frame: 0.004984000 seconds]
[Time since reference or first frame: 3.379730000 seconds]
Frame Number: 940
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37d7 (14295)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa516 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 51762, Dst Port: 53
Source Port: 51762
Destination Port: 53
Length: 41
Checksum: 0xc81c [unverified]
[Checksum Status: Unverified]
[Stream index: 27]
Domain Name System (query)
Transaction ID: 0xabe2
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... 0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
whereis.mit.edu: type A, class IN
Name: whereis.mit.edu
[Name Length: 15]

[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 941]

No.	Time	Source	Destination	Protocol	Length	Info
941	2018-10-17 16:36:33.624382	202.117.112.3	10.173.88.157	DNS	322	Standard query response

0xabe2 A whereis.mit.edu A 18.7.76.12 NS g.edu-servers.net NS c.edu-servers.net NS e.edu-servers.net NS d.edu-servers.net NS i.edu-servers.net NS k.edu-servers.net NS a.edu-servers.net NS h.edu-servers.net NS l.edu-servers.net NS f.edu-servers.net NS j.edu-servers.net NS b.edu-servers.net NS m.edu-servers.net

Frame 941: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.624382000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.624382000 seconds
[Time delta from previous captured frame: 0.001185000 seconds]
[Time delta from previous displayed frame: 0.001185000 seconds]
[Time since reference or first frame: 3.380915000 seconds]
Frame Number: 941
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
. 0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 300
Identification: 0x5200 (20992)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dfe [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 51762
Source Port: 53
Destination Port: 51762
Length: 280
Checksum: 0x9e24 [unverified]
[Checksum Status: Unverified]
[Stream index: 27]
Domain Name System (response)
Transaction ID: 0xabe2
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.0.... = Authoritative: Server is not an authority for domain

.... 0 = Truncated: Message is not truncated
.... 1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
.... 0... = Z: reserved (0)
.... 00. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 000 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

whereis.mit.edu: type A, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

whereis.mit.edu: type A, class IN, addr 18.7.76.12
 Name: whereis.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.7.76.12

Authoritative nameservers

edu: type NS, class IN, ns g.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 19
 Name Server: g.edu-servers.net

edu: type NS, class IN, ns c.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: c.edu-servers.net

edu: type NS, class IN, ns e.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: e.edu-servers.net

edu: type NS, class IN, ns d.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: d.edu-servers.net

edu: type NS, class IN, ns i.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: i.edu-servers.net

edu: type NS, class IN, ns k.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: k.edu-servers.net

edu: type NS, class IN, ns a.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172720
 Data length: 4
 Name Server: a.edu-servers.net

edu: type NS, class IN, ns h.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: h.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: m.edu-servers.net

[Request In: 940]
[Time: 0.001185000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
942	2018-10-17 16:36:33.631036	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x310f

AAAA whereis.mit.edu

Frame 942: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.631036000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.631036000 seconds
[Time delta from previous captured frame: 0.006654000 seconds]
[Time delta from previous displayed frame: 0.006654000 seconds]
[Time since reference or first frame: 3.387569000 seconds]
Frame Number: 942
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x000)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37d8 (14296)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa515 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 60591, Dst Port: 53
Source Port: 60591
Destination Port: 53
Length: 41
Checksum: 0x0573 [unverified]
[Checksum Status: Unverified]
[Stream index: 28]
Domain Name System (query)
Transaction ID: 0x310f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 whereis.mit.edu: type AAAA, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 950]
No. Time Source Destination Protocol Length Info
943 2018-10-17 16:36:33.631215 218.30.19.40 10.173.88.157 DNS 99 Standard query response
0xdf41 A whereis.mit.edu A 18.7.76.12
Frame 943: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.631215000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.631215000 seconds
[Time delta from previous captured frame: 0.000179000 seconds]
[Time delta from previous displayed frame: 0.000179000 seconds]
[Time since reference or first frame: 3.387748000 seconds]
Frame Number: 943
Frame Length: 99 bytes (792 bits)
Capture Length: 99 bytes (792 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)
 Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0. = LG bit: Globally unique address (factory default)
0 = IG bit: Individual address (unicast)
 Type: PPPoE Session (0x8864)
 PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 79
 Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 77
 Identification: 0x0000 (0)
 Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 57
 Protocol: UDP (17)
 Header checksum: 0xf10f [validation disabled]
 [Header checksum status: Unverified]
 Source: 218.30.19.40
 Destination: 10.173.88.157
 User Datagram Protocol, Src Port: 53, Dst Port: 50420
 Source Port: 53
 Destination Port: 50420
 Length: 57
 Checksum: 0x3867 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 25]
 Domain Name System (response)
 Transaction ID: 0xdf41
 Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0. = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 Queries
 whereis.mit.edu: type A, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 whereis.mit.edu: type A, class IN, addr 18.7.76.12
 Name: whereis.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.7.76.12
 [Request In: 937]
 [Time: 0.054930000 seconds]
 No. Time Source Destination Protocol Length Info
 946 2018-10-17 16:36:33.658743 218.30.19.40 10.173.88.157 DNS 79 Standard query response
 0xffe8 Server failure AAAA twitter.com

Frame 946: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.658743000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.658743000 seconds
[Time delta from previous captured frame: 0.011372000 seconds]
[Time delta from previous displayed frame: 0.027528000 seconds]
[Time since reference or first frame: 3.415276000 seconds]
Frame Number: 946
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf123 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61277
Source Port: 53
Destination Port: 61277
Length: 37
Checksum: 0x557f [unverified]
[Checksum Status: Unverified]
[Stream index: 15]
Domain Name System (response)
 Transaction ID: 0xffe8
Flags: 0x8182 Standard query response, Server failure
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0... = Z: reserved (0)
 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
 0.... = Non-authenticated data: Unacceptable
 0010 = Reply code: Server failure (2)
Questions: 1
Answer RRs: 0

Authority RRs: 0
Additional RRs: 0
Queries
 twitter.com: type AAAA, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Request In: 917]
 [Time: 0.194064000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
947	2018-10-17 16:36:33.659210	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xffe8

AAAA twitter.com
Frame 947: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.659210000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.659210000 seconds
[Time delta from previous captured frame: 0.000467000 seconds]
[Time delta from previous displayed frame: 0.000467000 seconds]
[Time since reference or first frame: 3.415743000 seconds]
Frame Number: 947
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37d9 (14297)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa518 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 61277, Dst Port: 53
 Source Port: 61277
 Destination Port: 53
 Length: 37
 Checksum: 0x88cf [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
Domain Name System (query)

Transaction ID: 0xffe8
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 911]
[DNS query retransmission. Original request in frame 911]
[Severity level: Warning]
[Group: Protocol]

Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
twitter.com: type AAAA, class IN
Name: twitter.com
[Name Length: 11]
[Label Count: 2]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

[Retransmitted request. Original request in: 911]
[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
949	2018-10-17 16:36:33.664931	10.173.88.157	218.30.19.40	DNS	83	Standard query 0x310f

AAAA whereis.mit.edu
Frame 949: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.664931000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.664931000 seconds
[Time delta from previous captured frame: 0.002951000 seconds]
[Time delta from previous displayed frame: 0.005721000 seconds]
[Time since reference or first frame: 3.421464000 seconds]
Frame Number: 949
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x6275 (25205)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7aa [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 60591, Dst Port: 53
Source Port: 60591
Destination Port: 53
Length: 41
Checksum: 0x52a5 [unverified]
[Checksum Status: Unverified]
[Stream index: 29]
Domain Name System (query)
Transaction ID: 0x310f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 whereis.mit.edu: type AAAA, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 951]
No. Time Source Destination Protocol Length Info
950 2018-10-17 16:36:33.694056 202.117.112.3 10.173.88.157 DNS 148 Standard query response
0x310f AAAA whereis.mit.edu use2.akam.net
Frame 950: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.694056000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.694056000 seconds
[Time delta from previous captured frame: 0.029125000 seconds]
[Time delta from previous displayed frame: 0.029125000 seconds]
[Time since reference or first frame: 3.450589000 seconds]
Frame Number: 950
Frame Length: 148 bytes (1184 bits)
Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 128
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 126
Identification: 0x5201 (20993)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8eab [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 60591
Source Port: 53
Destination Port: 60591
Length: 106
Checksum: 0x4b83 [unverified]
[Checksum Status: Unverified]
[Stream index: 28]

Domain Name System (response)
Transaction ID: 0x310f
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0... = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1... = Recursion available: Server can do recursive queries
.0... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0 = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
 whereis.mit.edu: type AAAA, class IN
 Name: whereis.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)

Authoritative nameservers
 mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 900
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)

[Request In: 942]
[Time: 0.063020000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
951	2018-10-17 16:36:33.694662	218.30.19.40	10.173.88.157	DNS	148	Standard query response

Frame 951: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.694662000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.694662000 seconds
[Time delta from previous captured frame: 0.000606000 seconds]
[Time delta from previous displayed frame: 0.000606000 seconds]
[Time since reference or first frame: 3.451195000 seconds]
Frame Number: 951
Frame Length: 148 bytes (1184 bits)

Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 128

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 126
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0de [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 60591
Source Port: 53
Destination Port: 60591
Length: 106
Checksum: 0x98b5 [unverified]
[Checksum Status: Unverified]
[Stream index: 29]

Domain Name System (response)
Transaction ID: 0x310f
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
whereis.mit.edu: type AAAA, class IN
Name: whereis.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
Name: mit.edu

Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 900
Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)
[Request In: 949]
[Time: 0.029731000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
952	2018-10-17 16:36:33.695021	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xdbdf

A web.mit.edu
Frame 952: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.695021000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.695021000 seconds
[Time delta from previous captured frame: 0.000359000 seconds]
[Time delta from previous displayed frame: 0.000359000 seconds]
[Time since reference or first frame: 3.451554000 seconds]
Frame Number: 952
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37da (14298)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
..0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa517 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 59498, Dst Port: 53
Source Port: 59498
Destination Port: 53
Length: 37
Checksum: 0x5ccb [unverified]
[Checksum Status: Unverified]

[Stream index: 30]
Domain Name System (query)
Transaction ID: 0xdbdf
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... ..0. = Z: reserved (0)
....0. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 web.mit.edu: type A, class IN
 Name: web.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 955]
No. Time Source Destination Protocol Length Info
953 2018-10-17 16:36:33.721589 10.173.88.157 218.30.19.40 DNS 79 Standard query 0xdbdf
A web.mit.edu
Frame 953: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.721589000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.721589000 seconds
[Time delta from previous captured frame: 0.026568000 seconds]
[Time delta from previous displayed frame: 0.026568000 seconds]
[Time since reference or first frame: 3.478122000 seconds]
Frame Number: 953
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x6276 (25206)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
.... 00.. = More fragments: Not set
.... 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7ad [validation disabled]

[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 59498, Dst Port: 53
Source Port: 59498
Destination Port: 53
Length: 37
Checksum: 0xa9fd [unverified]
[Checksum Status: Unverified]
[Stream index: 31]
Domain Name System (query)
Transaction ID: 0xdbdf
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 web.mit.edu: type A, class IN
 Name: web.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 956]
No. Time Source Destination Protocol Length Info
954 2018-10-17 16:36:33.735717 202.117.112.3 10.173.88.157 DNS 390 Standard query response
0x7f06 A news.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.26.244.21 NS j.gtld-servers.net NS
g.gtld-servers.net NS h.gtld-servers.net NS b.gtld-servers.net NS m.gtld-servers.net NS i.gtld-servers.net NS f.gtld-
servers.net NS a.gtld-servers.net NS l.gtld-servers.net NS c.gtld-servers.net NS k.gtld-servers.net NS e.gtld-servers.net NS
d.gtld-servers.net
Frame 954: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.735717000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.735717000 seconds
[Time delta from previous captured frame: 0.014128000 seconds]
[Time delta from previous displayed frame: 0.014128000 seconds]
[Time since reference or first frame: 3.492250000 seconds]
Frame Number: 954
Frame Length: 390 bytes (3120 bits)
Capture Length: 390 bytes (3120 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 370
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 368
Identification: 0x5202 (20994)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8db8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 56283
Source Port: 53
Destination Port: 56283
Length: 348
Checksum: 0x5fda [unverified]
[Checksum Status: Unverified]
[Stream index: 7]

Domain Name System (response)
Transaction ID: 0x7f06
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0. = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1... = Recursion available: Server can do recursive queries
.0... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0 = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 3
Authority RRs: 13
Additional RRs: 0
Queries
news.mit.edu: type A, class IN
Name: news.mit.edu
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
news.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
Name: news.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300
Data length: 25
CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dsrb.akamaiedge.net
Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 298
Data length: 24
CNAME: e9566.dsrb.akamaiedge.net
e9566.dsrb.akamaiedge.net: type A, class IN, addr 184.26.244.21
Name: e9566.dsrb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 298
Data length: 4
Address: 184.26.244.21

Authoritative nameservers
net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 17
Name Server: j.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net

Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: g.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: h.gtld-servers.net
net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: b.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: m.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: i.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: f.gtld-servers.net
net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: a.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: l.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: c.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: k.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net

Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: d.gtld-servers.net
[Request In: 905]
[Time: 0.312970000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
955	2018-10-17 16:36:33.754703	202.117.112.3	10.173.88.157	DNS	389	Standard query response

0xd8df A web.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 184.26.244.21 NS a.gtld-servers.net NS k.gtld-servers.net NS d.gtld-servers.net NS j.gtld-servers.net NS m.gtld-servers.net NS g.gtld-servers.net NS h.gtld-servers.net NS b.gtld-servers.net NS e.gtld-servers.net NS i.gtld-servers.net NS l.gtld-servers.net NS c.gtld-servers.net NS f.gtld-servers.net

Frame 955: 389 bytes on wire (3112 bits), 389 bytes captured (3112 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.754703000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.754703000 seconds
[Time delta from previous captured frame: 0.018986000 seconds]
[Time delta from previous displayed frame: 0.018986000 seconds]
[Time since reference or first frame: 3.511236000 seconds]
Frame Number: 955
Frame Length: 389 bytes (3112 bits)
Capture Length: 389 bytes (3112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 369
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 367
Identification: 0x5203 (20995)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8db8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 59498
Source Port: 53
Destination Port: 59498
Length: 347
Checksum: 0xda4b [unverified]
[Checksum Status: Unverified]
[Stream index: 30]
Domain Name System (response)

Transaction ID: 0xdbdf
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 13

Additional RRs: 0

Queries

web.mit.edu: type A, class IN
Name: web.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

web.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
Name: web.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800
Data length: 25
CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dsrb.akamaiedge.net
Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 298
Data length: 24
CNAME: e9566.dsrb.akamaiedge.net
e9566.dsrb.akamaiedge.net: type A, class IN, addr 184.26.244.21
Name: e9566.dsrb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 298
Data length: 4
Address: 184.26.244.21

Authoritative nameservers

net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 17
Name Server: a.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: k.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: d.gtld-servers.net
net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: j.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)

```

Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: m.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: g.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: h.gtld-servers.net
net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: b.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: i.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: l.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: c.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: f.gtld-servers.net

```

[Request In: 952]

[Time: 0.059682000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
956	2018-10-17 16:36:33.755709	218.30.19.40	10.173.88.157	DNS	168	Standard query response

0xdbdf A web.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.2.132.180

Frame 956: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.755709000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.755709000 seconds

[Time delta from previous captured frame: 0.001006000 seconds]

[Time delta from previous displayed frame: 0.001006000 seconds]

[Time since reference or first frame: 3.512242000 seconds]

Frame Number: 956

Frame Length: 168 bytes (1344 bits)

Capture Length: 168 bytes (1344 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 148

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 146
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0ca [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 59498
Source Port: 53
Destination Port: 59498
Length: 126
Checksum: 0x987e [unverified]
[Checksum Status: Unverified]
[Stream index: 31]

Domain Name System (response)
Transaction ID: 0xdbdf
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0

Queries
web.mit.edu: type A, class IN
Name: web.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
web.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
Name: web.mit.edu

Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800
Data length: 25
CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 298
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.2.132.180
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 298
Data length: 4
Address: 23.2.132.180
[Request In: 953]
[Time: 0.034120000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
957	2018-10-17 16:36:33.759006	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x21be

A careers.mit.edu
Frame 957: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.759006000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.759006000 seconds
[Time delta from previous captured frame: 0.003297000 seconds]
[Time delta from previous displayed frame: 0.003297000 seconds]
[Time since reference or first frame: 3.515539000 seconds]
Frame Number: 957
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37db (14299)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa512 [validation disabled]
[Header checksum status: Unverified]

Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 63153, Dst Port: 53
Source Port: 63153
Destination Port: 53
Length: 41
Checksum: 0x30c9 [unverified]
[Checksum Status: Unverified]
[Stream index: 32]
Domain Name System (query)
Transaction ID: 0x21be
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
careers.mit.edu: type A, class IN
 Name: careers.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 975]
No. Time Source Destination Protocol Length Info
958 2018-10-17 16:36:33.793192 10.173.88.157 218.30.19.40 DNS 83 Standard query 0x21be
A careers.mit.edu
Frame 958: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.793192000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.793192000 seconds
[Time delta from previous captured frame: 0.034186000 seconds]
[Time delta from previous displayed frame: 0.034186000 seconds]
[Time since reference or first frame: 3.549725000 seconds]
Frame Number: 958
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x6277 (25207)

Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a8 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 63153, Dst Port: 53
Source Port: 63153
Destination Port: 53
Length: 41
Checksum: 0x7dfb [unverified]
[Checksum Status: Unverified]
[Stream index: 33]
Domain Name System (query)
Transaction ID: 0x21be
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
careers.mit.edu: type A, class IN
 Name: careers.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 969]
No. Time Source Destination Protocol Length Info
969 2018-10-17 16:36:33.901652 218.30.19.40 10.173.88.157 DNS 127 Standard query response
0x21be A careers.mit.edu CNAME hr-prod-cms-2.mit.edu A 18.9.44.112
Frame 969: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.901652000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.901652000 seconds
[Time delta from previous captured frame: 0.040390000 seconds]
[Time delta from previous displayed frame: 0.108460000 seconds]
[Time since reference or first frame: 3.658185000 seconds]
Frame Number: 969
Frame Length: 127 bytes (1016 bits)
Capture Length: 127 bytes (1016 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 107
Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 105
 Identification: 0x0000 (0)
 Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 57
 Protocol: UDP (17)
 Header checksum: 0xf0f3 [validation disabled]
 [Header checksum status: Unverified]
 Source: 218.30.19.40
 Destination: 10.173.88.157
 User Datagram Protocol, Src Port: 53, Dst Port: 63153
 Source Port: 53
 Destination Port: 63153
 Length: 85
 Checksum: 0x936c [unverified]
 [Checksum Status: Unverified]
 [Stream index: 33]
 Domain Name System (response)
 Transaction ID: 0x21be
 Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0.... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1.... = Recursion available: Server can do recursive queries
 0.. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0 = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
 Questions: 1
 Answer RRs: 2
 Authority RRs: 0
 Additional RRs: 0
 Queries
 careers.mit.edu: type A, class IN
 Name: careers.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 careers.mit.edu: type CNAME, class IN, cname hr-prod-cms-2.mit.edu
 Name: careers.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 16
 CNAME: hr-prod-cms-2.mit.edu
 hr-prod-cms-2.mit.edu: type A, class IN, addr 18.9.44.112
 Name: hr-prod-cms-2.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.9.44.112
 [Request In: 958]
 [Time: 0.108460000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
970	2018-10-17 16:36:33.906708	10.173.88.157	202.117.112.3	DNS	89	Standard query 0x71a7

 A hr-prod-cms-2.mit.edu
 Frame 970: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:33.906708000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.906708000 seconds
[Time delta from previous captured frame: 0.005056000 seconds]
[Time delta from previous displayed frame: 0.005056000 seconds]
[Time since reference or first frame: 3.663241000 seconds]
Frame Number: 970
Frame Length: 89 bytes (712 bits)
Capture Length: 89 bytes (712 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 69
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 67
Identification: 0x37dc (14300)
Flags: 0x0000
0... = Reserved bit: Not set
.0. = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa50b [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 55518, Dst Port: 53
Source Port: 55518
Destination Port: 53
Length: 47
Checksum: 0x17e0 [unverified]
[Checksum Status: Unverified]
[Stream index: 34]
Domain Name System (query)
Transaction ID: 0x71a7
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
hr-prod-cms-2.mit.edu: type A, class IN
Name: hr-prod-cms-2.mit.edu
[Name Length: 21]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 974]

No.	Time	Source	Destination	Protocol	Length	Info
	973 2018-10-17 16:36:33.929709	10.173.88.157	218.30.19.40	DNS	89	Standard query 0x71a7
A hr-prod-cms-2.mit.edu						
Frame 973: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0						
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})						
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 17, 2018 16:36:33.929709000 中国标准时间						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1539765393.929709000 seconds						
[Time delta from previous captured frame: 0.007494000 seconds]						
[Time delta from previous displayed frame: 0.023001000 seconds]						
[Time since reference or first frame: 3.686242000 seconds]						
Frame Number: 973						
Frame Length: 89 bytes (712 bits)						
Capture Length: 89 bytes (712 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]						
[Coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
.... .0. = LG bit: Globally unique address (factory default)						
.... ..0. = IG bit: Individual address (unicast)						
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
.... .0. = LG bit: Globally unique address (factory default)						
.... ..0. = IG bit: Individual address (unicast)						
Type: PPPoE Session (0x8864)						
PPP-over-Ethernet Session						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Session Data (0x00)						
Session ID: 0x629d						
Payload Length: 69						
Point-to-Point Protocol						
Protocol: Internet Protocol version 4 (0x0021)						
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
0000 00.. = Differentiated Services Codepoint: Default (0)						
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
Total Length: 67						
Identification: 0x6278 (25208)						
Flags: 0x0000						
0... = Reserved bit: Not set						
.0... = Don't fragment: Not set						
..0. = More fragments: Not set						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0xc7a1 [validation disabled]						
[Header checksum status: Unverified]						
Source: 10.173.88.157						
Destination: 218.30.19.40						
User Datagram Protocol, Src Port: 55518, Dst Port: 53						
Source Port: 55518						
Destination Port: 53						
Length: 47						
Checksum: 0x6512 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 35]						
Domain Name System (query)						
Transaction ID: 0x71a7						
Flags: 0x0100 Standard query						
0... = Response: Message is a query						
.000 0... = Opcode: Standard query (0)						
.... ..0. = Truncated: Message is not truncated						
.... ...1 = Recursion desired: Do query recursively						
....0. = Z: reserved (0)						
....0 = Non-authenticated data: Unacceptable						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						

Additional RRs: 0
Queries

 hr-prod-cms-2.mit.edu: type A, class IN
 Name: hr-prod-cms-2.mit.edu
 [Name Length: 21]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 978]

No.	Time	Source	Destination	Protocol	Length	Info
974	2018-10-17 16:36:33.937389	202.117.112.3	10.173.88.157	DNS	328	Standard query response

0x71a7 A hr-prod-cms-2.mit.edu A 18.9.44.112 NS d.edu-servers.net NS k.edu-servers.net NS c.edu-servers.net NS a.edu-servers.net NS g.edu-servers.net NS b.edu-servers.net NS j.edu-servers.net NS f.edu-servers.net NS l.edu-servers.net NS h.edu-servers.net NS i.edu-servers.net NS e.edu-servers.net NS m.edu-servers.net

Frame 974: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.937389000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.937389000 seconds
[Time delta from previous captured frame: 0.007680000 seconds]
[Time delta from previous displayed frame: 0.007680000 seconds]
[Time since reference or first frame: 3.693922000 seconds]
Frame Number: 974
Frame Length: 328 bytes (2624 bits)
Capture Length: 328 bytes (2624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 308
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 306
Identification: 0x5204 (20996)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8df4 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55518
Source Port: 53
Destination Port: 55518
Length: 286
Checksum: 0x8474 [unverified]
[Checksum Status: Unverified]
[Stream index: 34]
Domain Name System (response)

Transaction ID: 0x71a7
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

hr-prod-cms-2.mit.edu: type A, class IN
Name: hr-prod-cms-2.mit.edu
[Name Length: 21]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

hr-prod-cms-2.mit.edu: type A, class IN, addr 18.9.44.112
Name: hr-prod-cms-2.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.44.112

Authoritative nameservers

edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 19
Name Server: d.edu-servers.net

edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: k.edu-servers.net

edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: c.edu-servers.net

edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: a.edu-servers.net

edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: g.edu-servers.net

edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: b.edu-servers.net

edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: h.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: i.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: m.edu-servers.net

[Request In: 970]
[Time: 0.030681000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
975	2018-10-17 16:36:33.937389	202.117.112.3	10.173.88.157	DNS	350	Standard query response

0x21be A careers.mit.edu CNAME hr-prod-cms-2.mit.edu A 18.9.44.112 NS c.edu-servers.net NS d.edu-servers.net NS j.edu-servers.net NS k.edu-servers.net NS g.edu-servers.net NS m.edu-servers.net NS b.edu-servers.net NS f.edu-servers.net NS h.edu-servers.net NS e.edu-servers.net NS l.edu-servers.net NS i.edu-servers.net NS a.edu-servers.net

Frame 975: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.937389000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.937389000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 3.693922000 seconds]
Frame Number: 975
Frame Length: 350 bytes (2800 bits)
Capture Length: 350 bytes (2800 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 330

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 328

Identification: 0x5205 (20997)

Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8ddd [validation disabled]
[Header checksum status: Unverified]

Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 63153
Source Port: 53
Destination Port: 63153
Length: 308

Checksum: 0xcdb4 [unverified]
[Checksum Status: Unverified]
[Stream index: 32]

Domain Name System (response)
Transaction ID: 0x21be

Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 2

Authority RRs: 13

Additional RRs: 0

Queries
careers.mit.edu: type A, class IN
Name: careers.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
careers.mit.edu: type CNAME, class IN, cname hr-prod-cms-2.mit.edu
Name: careers.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800
Data length: 16
CNAME: hr-prod-cms-2.mit.edu

hr-prod-cms-2.mit.edu: type A, class IN, addr 18.9.44.112
Name: hr-prod-cms-2.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.44.112

Authoritative nameservers

edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 19
Name Server: c.edu-servers.net

edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: d.edu-servers.net

edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: j.edu-servers.net

edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: k.edu-servers.net

edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: g.edu-servers.net

edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: m.edu-servers.net

edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: b.edu-servers.net

edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: f.edu-servers.net

edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: h.edu-servers.net

edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: e.edu-servers.net

edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4

Name Server: 1.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: i.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172720
Data length: 4
Name Server: a.edu-servers.net
[Request In: 957]
[Time: 0.178383000 seconds]
No. Time Source Destination Protocol Length Info
976 2018-10-17 16:36:33.940208 10.173.88.157 202.117.112.3 DNS 89 Standard query 0x1c2a
AAAA hr-prod-cms-2.mit.edu
Frame 976: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.940208000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.940208000 seconds
[Time delta from previous captured frame: 0.002819000 seconds]
[Time delta from previous displayed frame: 0.002819000 seconds]
[Time since reference or first frame: 3.696741000 seconds]
Frame Number: 976
Frame Length: 89 bytes (712 bits)
Capture Length: 89 bytes (712 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 69
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 67
Identification: 0x37dd (14301)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa50a [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 53237, Dst Port: 53
Source Port: 53237

Destination Port: 53
Length: 47
Checksum: 0x5b46 [unverified]
[Checksum Status: Unverified]
[Stream index: 36]
Domain Name System (query)
Transaction ID: 0x1c2a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 hr-prod-cms-2.mit.edu: type AAAA, class IN
 Name: hr-prod-cms-2.mit.edu
 [Name Length: 21]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 979]
No. Time Source Destination Protocol Length Info
977 2018-10-17 16:36:33.965721 10.173.88.157 218.30.19.40 DNS 89 Standard query 0x1c2a
AAAA hr-prod-cms-2.mit.edu
Frame 977: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:33:965721000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.965721000 seconds
[Time delta from previous captured frame: 0.025513000 seconds]
[Time delta from previous displayed frame: 0.025513000 seconds]
[Time since reference or first frame: 3.722254000 seconds]
Frame Number: 977
Frame Length: 89 bytes (712 bits)
Capture Length: 89 bytes (712 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:etherype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 69
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 67
Identification: 0x6279 (25209)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a0 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 53237, Dst Port: 53
Source Port: 53237
Destination Port: 53
Length: 47
Checksum: 0xa878 [unverified]
[Checksum Status: Unverified]
[Stream index: 37]
Domain Name System (query)
Transaction ID: 0x1c2a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0.. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 hr-prod-cms-2.mit.edu: type AAAA, class IN
 Name: hr-prod-cms-2.mit.edu
 [Name Length: 21]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 987]
No. Time Source Destination Protocol Length Info
978 2018-10-17 16:36:33.987479 218.30.19.40 10.173.88.157 DNS 105 Standard query response
0x71a7 A hr-prod-cms-2.mit.edu A 18.9.44.112
Frame 978: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.987479000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.987479000 seconds
[Time delta from previous captured frame: 0.021758000 seconds]
[Time delta from previous displayed frame: 0.021758000 seconds]
[Time since reference or first frame: 3.744012000 seconds]
Frame Number: 978
Frame Length: 105 bytes (840 bits)
Capture Length: 105 bytes (840 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 85
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.0 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 83

Identification: 0x0000 (0)

Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 57

Protocol: UDP (17)

Header checksum: 0xf109 [validation disabled]
[Header checksum status: Unverified]

Source: 218.30.19.40

Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 55518
Source Port: 53
Destination Port: 55518
Length: 63
Checksum: 0x506b [unverified]
[Checksum Status: Unverified]
[Stream index: 35]

Domain Name System (response)
Transaction ID: 0x71a7
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.0. = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
.0.... = Z: reserved (0)
.0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
.0.... = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
hr-prod-cms-2.mit.edu: type A, class IN
Name: hr-prod-cms-2.mit.edu
[Name Length: 21]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
hr-prod-cms-2.mit.edu: type A, class IN, addr 18.9.44.112
Name: hr-prod-cms-2.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.44.112
[Request In: 973]
[Time: 0.057770000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
979	2018-10-17 16:36:33.994366	202.117.112.3	10.173.88.157	DNS	154	Standard query response

Frame 979: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.994366000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.994366000 seconds
[Time delta from previous captured frame: 0.006887000 seconds]
[Time delta from previous displayed frame: 0.006887000 seconds]
[Time since reference or first frame: 3.750899000 seconds]
Frame Number: 979
Frame Length: 154 bytes (1232 bits)
Capture Length: 154 bytes (1232 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 134

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 132

Identification: 0x5206 (20998)

Flags: 0x0000

0... = Reserved bit: Not set

.0... = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8ea0 [validation disabled]

[Header checksum status: Unverified]

Source: 202.117.112.3

Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 53237

Source Port: 53

Destination Port: 53237

Length: 112

Checksum: 0x174d [unverified]

[Checksum Status: Unverified]

[Stream index: 36]

Domain Name System (response)

Transaction ID: 0x1c2a

Flags: 0x8180 Standard query response, No error

1.... = Response: Message is a response

.000 0... = Opcode: Standard query (0)

.... .0... = Authoritative: Server is not an authority for domain

.... ..0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively

.... 1.... = Recursion available: Server can do recursive queries

....0... = Z: reserved (0)

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server

....0 = Non-authenticated data: Unacceptable

.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

hr-prod-cms-2.mit.edu: type AAAA, class IN

Name: hr-prod-cms-2.mit.edu

[Name Length: 21]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Authoritative nameservers

mit.edu: type SOA, class IN, mname use2.akam.net

Name: mit.edu

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 1800

Data length: 53

Primary name server: use2.akam.net

Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)

[Request In: 976]
[Time: 0.054158000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
980	2018-10-17 16:36:33.995740	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x3afa

A www.youtube.com

Frame 980: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.995740000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.995740000 seconds
[Time delta from previous captured frame: 0.001374000 seconds]
[Time delta from previous displayed frame: 0.001374000 seconds]
[Time since reference or first frame: 3.752273000 seconds]
Frame Number: 980
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37de (14302)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa50f [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 54140, Dst Port: 53
Source Port: 54140
Destination Port: 53
Length: 41
Checksum: 0x14a4 [unverified]
[Checksum Status: Unverified]
[Stream index: 38]
Domain Name System (query)
Transaction ID: 0x3afa
Flags: 0x0100 Standard query
0... = Response: Message is a query

.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.youtube.com: type A, class IN

Name: www.youtube.com

[Name Length: 15]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 981]

No.	Time	Source	Destination	Protocol	Length	Info
981	2018-10-17 16:36:33.996478	202.117.112.3	10.173.88.157	DNS	412	Standard query response

0x3afa A www.youtube.com CNAME youtube-ui.l.google.com CNAME youtube-ui-china.l.google.com A 67.228.126.62 NS ns2.google.com
NS ns4.google.com NS ns3.google.com NS ns1.google.com A 216.239.32.10 AAAA 2001:4860:4802:32::a A 216.239.34.10 AAAA
2001:4860:4802:34::a A 216.239.36.10 AAAA 2001:4860:4802:36::a A 216.239.38.10 AAAA 2001:4860:4802:38::a

Frame 981: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.996478000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.996478000 seconds

[Time delta from previous captured frame: 0.000738000 seconds]

[Time delta from previous displayed frame: 0.000738000 seconds]

[Time since reference or first frame: 3.753011000 seconds]

Frame Number: 981

Frame Length: 412 bytes (3296 bits)

Capture Length: 412 bytes (3296 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 392

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 390

Identification: 0x5207 (20999)

Flags: 0x0000

0... = Reserved bit: Not set

.0... = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8d9d [validation disabled]

[Header checksum status: Unverified]

Source: 202.117.112.3

Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 54140
Source Port: 53
Destination Port: 54140
Length: 370
Checksum: 0xb42 [unverified]
[Checksum Status: Unverified]
[Stream index: 38]
Domain Name System (response)
Transaction ID: 0x3afa
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 4
Additional RRs: 8
Queries
www.youtube.com: type A, class IN
Name: www.youtube.com
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
Name: www.youtube.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 83130
Data length: 22
CNAME: youtube-ui.l.google.com
youtube-ui.l.google.com: type CNAME, class IN, cname youtube-ui-china.l.google.com
Name: youtube-ui.l.google.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 584
Data length: 19
CNAME: youtube-ui-china.l.google.com
youtube-ui-china.l.google.com: type A, class IN, addr 67.228.126.62
Name: youtube-ui-china.l.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 215
Data length: 4
Address: 67.228.126.62
Authoritative nameservers
google.com: type NS, class IN, ns ns2.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns2.google.com
google.com: type NS, class IN, ns ns4.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns4.google.com
google.com: type NS, class IN, ns ns3.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns3.google.com
google.com: type NS, class IN, ns ns1.google.com
Name: google.com

Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 171639
 Data length: 6
 Name Server: ns1.google.com

Additional records

ns1.google.com: type A, class IN, addr 216.239.32.10
 Name: ns1.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 251764
 Data length: 4
 Address: 216.239.32.10

ns1.google.com: type AAAA, class IN, addr 2001:4860:4802:32::a
 Name: ns1.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 251767
 Data length: 16
 AAAA Address: 2001:4860:4802:32::a

ns2.google.com: type A, class IN, addr 216.239.34.10
 Name: ns2.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 251766
 Data length: 4
 Address: 216.239.34.10

ns2.google.com: type AAAA, class IN, addr 2001:4860:4802:34::a
 Name: ns2.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 278431
 Data length: 16
 AAAA Address: 2001:4860:4802:34::a

ns3.google.com: type A, class IN, addr 216.239.36.10
 Name: ns3.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 167608
 Data length: 4
 Address: 216.239.36.10

ns3.google.com: type AAAA, class IN, addr 2001:4860:4802:36::a
 Name: ns3.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 251770
 Data length: 16
 AAAA Address: 2001:4860:4802:36::a

ns4.google.com: type A, class IN, addr 216.239.38.10
 Name: ns4.google.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 251764
 Data length: 4
 Address: 216.239.38.10

ns4.google.com: type AAAA, class IN, addr 2001:4860:4802:38::a
 Name: ns4.google.com
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 Time to live: 167755
 Data length: 16
 AAAA Address: 2001:4860:4802:38::a

[Request In: 980]
[Time: 0.000738000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
	982 2018-10-17 16:36:33.997238	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x6067

AAAA www.youtube.com

Frame 982: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:33.997238000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765393.997238000 seconds

[Time delta from previous captured frame: 0.000760000 seconds]
[Time delta from previous displayed frame: 0.000760000 seconds]
[Time since reference or first frame: 3.753771000 seconds]

Frame Number: 982
 Frame Length: 83 bytes (664 bits)
 Capture Length: 83 bytes (664 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:etherype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 63

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 61
 Identification: 0x37df (14303)
 Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa50e [validation disabled]
 [Header checksum status: Unverified]

Source: 10.173.88.157
 Destination: 202.117.112.3

User Datagram Protocol, Src Port: 51142, Dst Port: 53
 Source Port: 51142
 Destination Port: 53
 Length: 41
 Checksum: 0xdfec [unverified]
 [Checksum Status: Unverified]
 [Stream index: 39]

Domain Name System (query)
 Transaction ID: 0x6067
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0. = Z: reserved (0)
0 = Non-authenticated data: Unacceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.youtube.com: type AAAA, class IN
 Name: www.youtube.com
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)

[Response In: 983]

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

983 2018-10-17 16:36:33.997936 202.117.112.3 10.173.88.157 DNS 424 Standard query response
0x6067 AAAA www.youtube.com CNAME youtube-ui.1.google.com CNAME youtube-ui-china.1.google.com AAAA
2400:cb00:2048:1::6814:224e NS ns4.google.com NS ns1.google.com NS ns3.google.com NS ns2.google.com A 216.239.32.10 AAAA
2001:4860:4802:32::a A 216.239.34.10 AAAA 2001:4860:4802:34::a A 216.239.36.10 AAAA 2001:4860:4802:36::a A 216.239.38.10
AAAA 2001:4860:4802:38::a

Frame 983: 424 bytes on wire (3392 bits), 424 bytes captured (3392 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.997936000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.997936000 seconds
[Time delta from previous captured frame: 0.000698000 seconds]
[Time delta from previous displayed frame: 0.000698000 seconds]
[Time since reference or first frame: 3.754469000 seconds]
Frame Number: 983
Frame Length: 424 bytes (3392 bits)
Capture Length: 424 bytes (3392 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 404

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 402
Identification: 0x5208 (21000)
Flags: 0x0000
.... = Reserved bit: Not set
.0. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8d90 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 51142
Source Port: 53
Destination Port: 51142
Length: 382
Checksum: 0x4e52 [unverified]
[Checksum Status: Unverified]
[Stream index: 39]

Domain Name System (response)
Transaction ID: 0x6067
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 4

Additional RRs: 8

Queries

www.youtube.com: type AAAA, class IN
Name: www.youtube.com
[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Answers

www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
Name: www.youtube.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 83130
Data length: 22
CNAME: youtube-ui.l.google.com

youtube-ui.l.google.com: type CNAME, class IN, cname youtube-ui-china.l.google.com
Name: youtube-ui.l.google.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 584
Data length: 19
CNAME: youtube-ui-china.l.google.com

youtube-ui-china.l.google.com: type AAAA, class IN, addr 2400:cb00:2048:1::6814:224e
Name: youtube-ui-china.l.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 231
Data length: 16
AAAA Address: 2400:cb00:2048:1::6814:224e

Authoritative nameservers

google.com: type NS, class IN, ns ns4.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns4.google.com

google.com: type NS, class IN, ns ns1.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns1.google.com

google.com: type NS, class IN, ns ns3.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns3.google.com

google.com: type NS, class IN, ns ns2.google.com
Name: google.com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 171639
Data length: 6
Name Server: ns2.google.com

Additional records

ns1.google.com: type A, class IN, addr 216.239.32.10
Name: ns1.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 251764
Data length: 4
Address: 216.239.32.10

ns1.google.com: type AAAA, class IN, addr 2001:4860:4802:32::a
Name: ns1.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Time to live: 251767
Data length: 16
AAAA Address: 2001:4860:4802:32::a
ns2.google.com: type A, class IN, addr 216.239.34.10
Name: ns2.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 251766
Data length: 4
Address: 216.239.34.10
ns2.google.com: type AAAA, class IN, addr 2001:4860:4802:34::a
Name: ns2.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 278431
Data length: 16
AAAA Address: 2001:4860:4802:34::a
ns3.google.com: type A, class IN, addr 216.239.36.10
Name: ns3.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 167608
Data length: 4
Address: 216.239.36.10
ns3.google.com: type AAAA, class IN, addr 2001:4860:4802:36::a
Name: ns3.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 251770
Data length: 16
AAAA Address: 2001:4860:4802:36::a
ns4.google.com: type A, class IN, addr 216.239.38.10
Name: ns4.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 251764
Data length: 4
Address: 216.239.38.10
ns4.google.com: type AAAA, class IN, addr 2001:4860:4802:38::a
Name: ns4.google.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 167755
Data length: 16
AAAA Address: 2001:4860:4802:38::a
[Request In: 982]
[Time: 0.000698000 seconds]
No. Time Source Destination Protocol Length Info
984 2018-10-17 16:36:33.999010 10.173.88.157 202.117.112.3 DNS 85 Standard query 0x5426
A www.instagram.com
Frame 984: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.999010000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.999010000 seconds
[Time delta from previous captured frame: 0.001074000 seconds]
[Time delta from previous displayed frame: 0.001074000 seconds]
[Time since reference or first frame: 3.755543000 seconds]
Frame Number: 984
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37e0 (14304)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa50b [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 56440, Dst Port: 53
Source Port: 56440
Destination Port: 53
Length: 43
Checksum: 0x8b23 [unverified]
[Checksum Status: Unverified]
[Stream index: 40]
Domain Name System (query)
Transaction ID: 0x5426
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... 00. = Truncated: Message is not truncated
.... 01 = Recursion desired: Do query recursively
.... 00. = Z: reserved (0)
.... 00. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type A, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 985]
No. Time Source Destination Protocol Length Info
985 2018-10-17 16:36:33.999926 202.117.112.3 10.173.88.157 DNS 325 Standard query response
0x5426 A www.instagram.com A 203.98.7.65 NS d.gtld-servers.net NS a.gtld-servers.net NS h.gtld-servers.net NS b.gtld-servers.net NS j.gtld-servers.net NS e.gtld-servers.net NS f.gtld-servers.net NS k.gtld-servers.net NS m.gtld-servers.net NS i.gtld-servers.net NS l.gtld-servers.net NS c.gtld-servers.net NS g.gtld-servers.net
Frame 985: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:33.999926000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765393.999926000 seconds
[Time delta from previous captured frame: 0.000916000 seconds]
[Time delta from previous displayed frame: 0.000916000 seconds]
[Time since reference or first frame: 3.756459000 seconds]
Frame Number: 985
Frame Length: 325 bytes (2600 bits)
Capture Length: 325 bytes (2600 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 305

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 303
Identification: 0x5209 (21001)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8df2 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 56440
Source Port: 53
Destination Port: 56440
Length: 283
Checksum: 0x7835 [unverified]
[Checksum Status: Unverified]
[Stream index: 40]

Domain Name System (response)
Transaction ID: 0x5426
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
www.instagram.com: type A, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
www.instagram.com: type A, class IN, addr 203.98.7.65
Name: www.instagram.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 163
Data length: 4

Address: 203.98.7.65

Authoritative nameservers

com: type NS, class IN, ns d.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 20
Name Server: d.gtld-servers.net
com: type NS, class IN, ns a.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: a.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: h.gtld-servers.net
com: type NS, class IN, ns b.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: b.gtld-servers.net
com: type NS, class IN, ns j.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: j.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: e.gtld-servers.net
com: type NS, class IN, ns f.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: f.gtld-servers.net
com: type NS, class IN, ns k.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: k.gtld-servers.net
com: type NS, class IN, ns m.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: m.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: i.gtld-servers.net
com: type NS, class IN, ns l.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182

Data length: 4
Name Server: 1.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: c.gtld-servers.net
com: type NS, class IN, ns g.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169182
Data length: 4
Name Server: g.gtld-servers.net
[Request In: 984]
[Time: 0.000916000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
986	2018-10-17 16:36:34.000802	10.173.88.157	202.117.112.3	DNS	85	Standard query 0xd571

AAAA www.instagram.com
Frame 986: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.000802000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.000802000 seconds
[Time delta from previous captured frame: 0.000876000 seconds]
[Time delta from previous displayed frame: 0.000876000 seconds]
[Time since reference or first frame: 3.757335000 seconds]
Frame Number: 986
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37e1 (14305)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa50a [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 64089, Dst Port: 53

Source Port: 64089
Destination Port: 53
Length: 43
Checksum: 0xd0f6 [unverified]
[Checksum Status: Unverified]
[Stream index: 41]
Domain Name System (query)
Transaction ID: 0xd571
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type AAAA, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1573]
No. Time Source Destination Protocol Length Info
987 2018-10-17 16:36:34.019598 218.30.19.40 10.173.88.157 DNS 154 Standard query response
0x1c2a AAAA hr-prod-cms-2.mit.edu SOA use2.akam.net
Frame 987: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.019598000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.019598000 seconds
[Time delta from previous captured frame: 0.018796000 seconds]
[Time delta from previous displayed frame: 0.018796000 seconds]
[Time since reference or first frame: 3.776131000 seconds]
Frame Number: 987
Frame Length: 154 bytes (1232 bits)
Capture Length: 154 bytes (1232 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 134
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 132
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set

..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0d8 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 53237
Source Port: 53
Destination Port: 53237
Length: 112
Checksum: 0x647f [unverified]
[Checksum Status: Unverified]
[Stream index: 37]
Domain Name System (response)
Transaction ID: 0x1c2a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
 hr-prod-cms-2.mit.edu: type AAAA, class IN
 Name: hr-prod-cms-2.mit.edu
 [Name Length: 21]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
Authoritative nameservers
 mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)
 [Request In: 977]
 [Time: 0.053877000 seconds]
No. Time Source Destination Protocol Length Info
988 2018-10-17 16:36:34.024696 10.173.88.157 218.30.19.40 DNS 85 Standard query 0xd571
AAAA www.instagram.com
Frame 988: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.024696000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.024696000 seconds
[Time delta from previous captured frame: 0.005098000 seconds]
[Time delta from previous displayed frame: 0.005098000 seconds]
[Time since reference or first frame: 3.781229000 seconds]
Frame Number: 988
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x627a (25210)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a3 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 64089, Dst Port: 53
Source Port: 64089
Destination Port: 53
Length: 43
Checksum: 0x1e29 [unverified]
[Checksum Status: Unverified]
[Stream index: 42]

Domain Name System (query)
Transaction ID: 0xd571
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... 0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... 0.... = Z: reserved (0)
.... 0.... = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type AAAA, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1013]

No.	Time	Source	Destination	Protocol	Length	Info
1009	2018-10-17 16:36:34.131269	10.173.88.157	202.117.112.3	DNS	95	Standard query 0xbb54

A siteintercept.qualtrics.com
Frame 1009: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:34.131269000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.131269000 seconds
[Time delta from previous captured frame: 0.028742000 seconds]
[Time delta from previous displayed frame: 0.106573000 seconds]
[Time since reference or first frame: 3.887802000 seconds]

Frame Number: 1009
 Frame Length: 95 bytes (760 bits)
 Capture Length: 95 bytes (760 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:etherype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 75

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 73
 Identification: 0x37e2 (14306)
 Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa4ff [validation disabled]
 [Header checksum status: Unverified]

Source: 10.173.88.157
 Destination: 202.117.112.3

User Datagram Protocol, Src Port: 61001, Dst Port: 53
 Source Port: 61001
 Destination Port: 53
 Length: 53
 Checksum: 0xfc6 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 43]

Domain Name System (query)
 Transaction ID: 0xbb54
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0. = Z: reserved (0)
0 = Non-authenticated data: Unacceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 siteintercept.qualtrics.com: type A, class IN
 Name: siteintercept.qualtrics.com
 [Name Length: 27]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

[Response In: 1010]

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

1010 2018-10-17 16:36:34.132171 202.117.112.3 10.173.88.157 DNS 412 Standard query response
0xbb54 A siteintercept.qualtrics.com CNAME cloud.qualtrics.com.edgekey.net CNAME e3672.ksd.akamaiedge.net A 23.11.246.32 NS
m.gtld-servers.net NS h.gtld-servers.net NS j.gtld-servers.net NS b.gtld-servers.net NS d.gtld-servers.net NS k.gtld-
servers.net NS l.gtld-servers.net NS c.gtld-servers.net NS a.gtld-servers.net NS f.gtld-servers.net NS e.gtld-servers.net NS
g.gtld-servers.net NS i.gtld-servers.net
Frame 1010: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.132171000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.132171000 seconds
[Time delta from previous captured frame: 0.000902000 seconds]
[Time delta from previous displayed frame: 0.000902000 seconds]
[Time since reference or first frame: 3.888704000 seconds]
Frame Number: 1010
Frame Length: 412 bytes (3296 bits)
Capture Length: 412 bytes (3296 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 392
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 390
Identification: 0x520a (21002)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0xd9a [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61001
Source Port: 53
Destination Port: 61001
Length: 370
Checksum: 0x0089 [unverified]
[Checksum Status: Unverified]
[Stream index: 43]
Domain Name System (response)
Transaction ID: 0xbb54
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 13

Additional RRs: 0

Queries

siteintercept.qualtrics.com: type A, class IN
Name: siteintercept.qualtrics.com
[Name Length: 27]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

siteintercept.qualtrics.com: type CNAME, class IN, cname cloud.qualtrics.com.edgekey.net

Name: siteintercept.qualtrics.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1846
Data length: 33

CNAME: cloud.qualtrics.com.edgekey.net

cloud.qualtrics.com.edgekey.net: type CNAME, class IN, cname e3672.ksd.akamaiedge.net

Name: cloud.qualtrics.com.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 191
Data length: 23

CNAME: e3672.ksd.akamaiedge.net

e3672.ksd.akamaiedge.net: type A, class IN, addr 23.11.246.32

Name: e3672.ksd.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 191
Data length: 4

Address: 23.11.246.32

Authoritative nameservers

net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 17

Name Server: m.gtld-servers.net

net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4

Name Server: h.gtld-servers.net

net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4

Name Server: j.gtld-servers.net

net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4

Name Server: b.gtld-servers.net

net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4

Name Server: d.gtld-servers.net

net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189

Name Server: k.gtld-servers.net

```
Data length: 4
Name Server: k.gtld-servers.net
net: type NS, class IN, ns 1.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: 1.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: c.gtld-servers.net
net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: a.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: f.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: g.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169189
Data length: 4
Name Server: i.gtld-servers.net
[Request In: 1009]
[Time: 0.000902000 seconds]
No. Time Source Destination Protocol Length Info
1013 2018-10-17 16:36:34.228083 218.30.19.40 10.173.88.157 DNS 85 Standard query response
0xd571 Server failure AAAA www.instagram.com
Frame 1013: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.228083000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.228083000 seconds
[Time delta from previous captured frame: 0.090057000 seconds]
[Time delta from previous displayed frame: 0.095912000 seconds]
[Time since reference or first frame: 3.984616000 seconds]
Frame Number: 1013
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
```

.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf11d [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 64089
Source Port: 53
Destination Port: 64089
Length: 43
Checksum: 0x9da6 [unverified]
[Checksum Status: Unverified]
[Stream index: 42]

Domain Name System (response)
Transaction ID: 0xd571
Flags: 0x8182 Standard query response, Server failure
 1... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0.. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0.. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0. = Non-authenticated data: Unacceptable
 0010 = Reply code: Server failure (2)

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries
 www.instagram.com: type AAAA, class IN
 Name: www.instagram.com
 [Name Length: 17]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Request In: 988]
 [Time: 0.203387000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1014	2018-10-17 16:36:34.228305	10.173.88.157	202.117.112.3	DNS	85	Standard query 0xd571

AAAA www.instagram.com
Frame 1014: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.228305000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.228305000 seconds

[Time delta from previous captured frame: 0.000222000 seconds]
[Time delta from previous displayed frame: 0.000222000 seconds]
[Time since reference or first frame: 3.984838000 seconds]
Frame Number: 1014
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37e3 (14307)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa508 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 64089, Dst Port: 53
Source Port: 64089
Destination Port: 53
Length: 43
Checksum: 0xd0f6 [unverified]
[Checksum Status: Unverified]
[Stream index: 41]
Domain Name System (query)
Transaction ID: 0xd571
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 986]
[DNS query retransmission. Original request in frame 986]
[Severity level: Warning]
[Group: Protocol]
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type AAAA, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]

Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Retransmitted request. Original request in: 986]
[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
1031	2018-10-17 16:36:34.607837	10.173.88.157	202.117.112.3	DNS	84	Standard query 0x1494

A calendar.mit.edu

Frame 1031: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.607837000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.607837000 seconds
[Time delta from previous captured frame: 0.075435000 seconds]
[Time delta from previous displayed frame: 0.379532000 seconds]
[Time since reference or first frame: 4.364370000 seconds]
Frame Number: 1031
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.0 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37e4 (14308)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa508 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 57780, Dst Port: 53
Source Port: 57780
Destination Port: 53
Length: 42
Checksum: 0x08e2 [unverified]
[Checksum Status: Unverified]
[Stream index: 24]

Domain Name System (query)
Transaction ID: 0x1494
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 936]
[DNS query retransmission. Original request in frame 936]
[Severity level: Warning]
[Group: Protocol]
Flags: 0x0100 Standard query
0.... = Response: Message is a query

.000 0... = Opcode: Standard query (0)
. 0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 calendar.mit.edu: type A, class IN
 Name: calendar.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
[Retransmitted request. Original request in: 936]
[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
1360	2018-10-17 16:36:34.831546	218.30.19.40	10.173.88.157	DNS	141	Standard query response

Frame 1360: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.831546000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.831546000 seconds
[Time delta from previous captured frame: 0.003243000 seconds]
[Time delta from previous displayed frame: 0.223709000 seconds]
[Time since reference or first frame: 4.588079000 seconds]
Frame Number: 1360
Frame Length: 141 bytes (1128 bits)
Capture Length: 141 bytes (1128 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 121
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 119
 Identification: 0x0000 (0)
 Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1... = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 57
 Protocol: UDP (17)
 Header checksum: 0xf0e5 [validation disabled]
 [Header checksum status: Unverified]
 Source: 218.30.19.40
 Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 57780

Source Port: 53
Destination Port: 57780
Length: 99
Checksum: 0xbc7d [unverified]
[Checksum Status: Unverified]
[Stream index: 26]
Domain Name System (response)
Transaction ID: 0x1494
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0... = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
.0... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0 = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
calendar.mit.edu: type A, class IN
 Name: calendar.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
calendar.mit.edu: type CNAME, class IN, cname mit.enterprise.localist.com
 Name: calendar.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 29
 CNAME: mit.enterprise.localist.com
mit.enterprise.localist.com: type A, class IN, addr 199.19.67.172
 Name: mit.enterprise.localist.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1200
 Data length: 4
 Address: 199.19.67.172
[Request In: 938]
[Time: 1.254196000 seconds]
No. Time Source Destination Protocol Length Info
1367 2018-10-17 16:36:34.835097 10.173.88.157 202.117.112.3 DNS 95 Standard query 0x1609
A mit.enterprise.localist.com
Frame 1367: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.835097000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.835097000 seconds
[Time delta from previous captured frame: 0.002884000 seconds]
[Time delta from previous displayed frame: 0.003551000 seconds]
[Time since reference or first frame: 4.591630000 seconds]
Frame Number: 1367
Frame Length: 95 bytes (760 bits)
Capture Length: 95 bytes (760 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
 PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 75
 Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 73
 Identification: 0x37e5 (14309)
 Flags: 0x0000
 0.... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa4fc [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.173.88.157
 Destination: 202.117.112.3
 User Datagram Protocol, Src Port: 63833, Dst Port: 53
 Source Port: 63833
 Destination Port: 53
 Length: 53
 Checksum: 0xa28d [unverified]
 [Checksum Status: Unverified]
 [Stream index: 44]
 Domain Name System (query)
 Transaction ID: 0x1609
 Flags: 0x0100 Standard query
 0.... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0... = Z: reserved (0)
0 = Non-authenticated data: Unacceptable
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 mit.enterprise.localist.com: type A, class IN
 Name: mit.enterprise.localist.com
 [Name Length: 27]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1516]

No.	Time	Source	Destination	Protocol	Length	Info
1412	2018-10-17 16:36:34.864778	10.173.88.157	218.30.19.40	DNS	95	Standard query 0x1609

 A mit.enterprise.localist.com
 Frame 1412: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:34.864778000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765394.864778000 seconds
 [Time delta from previous captured frame: 0.004122000 seconds]
 [Time delta from previous displayed frame: 0.029681000 seconds]
 [Time since reference or first frame: 4.621311000 seconds]
 Frame Number: 1412
 Frame Length: 95 bytes (760 bits)
 Capture Length: 95 bytes (760 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 75
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 73
Identification: 0x627b (25211)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc798 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 63833, Dst Port: 53
Source Port: 63833
Destination Port: 53
Length: 53
Checksum: 0xefbf [unverified]
[Checksum Status: Unverified]
[Stream index: 45]
Domain Name System (query)
Transaction ID: 0x1609
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.enterprise.localist.com: type A, class IN
Name: mit.enterprise.localist.com
[Name Length: 27]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1426]
No. Time Source Destination Protocol Length Info
1426 2018-10-17 16:36:34.870247 218.30.19.40 10.173.88.157 DNS 111 Standard query response
0x1609 A mit.enterprise.localist.com A 199.19.67.172
Frame 1426: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.870247000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.870247000 seconds
[Time delta from previous captured frame: 0.000002000 seconds]
[Time delta from previous displayed frame: 0.005469000 seconds]

[Time since reference or first frame: 4.626780000 seconds]
Frame Number: 1426
Frame Length: 111 bytes (888 bits)
Capture Length: 111 bytes (888 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ether type:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 91
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 89
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf103 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 63833
Source Port: 53
Destination Port: 63833
Length: 69
Checksum: 0xec4e [unverified]
[Checksum Status: Unverified]
[Stream index: 45]
Domain Name System (response)
Transaction ID: 0x1609
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0.... = Opcode: Standard query (0)
 0.. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1.... = Recursion available: Server can do recursive queries
 0.. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0 = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
 mit.enterprise.localist.com: type A, class IN
 Name: mit.enterprise.localist.com
 [Name Length: 27]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

mit.enterprise.localist.com: type A, class IN, addr 199.19.67.172
Name: mit.enterprise.localist.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1200
Data length: 4
Address: 199.19.67.172
[Request In: 1412]
[Time: 0.005469000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1429	2018-10-17 16:36:34.872300	10.173.88.157	202.117.112.3	DNS	95	Standard query 0xc9f7

AAAA mit.enterprise.localist.com
Frame 1429: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.872300000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.872300000 seconds
[Time delta from previous captured frame: 0.001366000 seconds]
[Time delta from previous displayed frame: 0.002053000 seconds]
[Time since reference or first frame: 4.628833000 seconds]
Frame Number: 1429
Frame Length: 95 bytes (760 bits)
Capture Length: 95 bytes (760 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.0. = LG bit: Globally unique address (factory default)
.0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.0. = LG bit: Globally unique address (factory default)
.0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 75
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 73
Identification: 0x37e6 (14310)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fb [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 53192, Dst Port: 53
Source Port: 53192
Destination Port: 53
Length: 53
Checksum: 0xfd2f [unverified]
[Checksum Status: Unverified]
[Stream index: 46]
Domain Name System (query)
Transaction ID: 0xc9f7

Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.enterprise.localist.com: type AAAA, class IN
Name: mit.enterprise.localist.com
[Name Length: 27]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

[Response In: 1498]

No.	Time	Source	Destination	Protocol	Length	Info
1476	2018-10-17 16:36:34.904778	10.173.88.157	218.30.19.40	DNS	95	Standard query 0xc9f7

AAAA mit.enterprise.localist.com

Frame 1476: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:34.904778000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765394.904778000 seconds
[Time delta from previous captured frame: 0.003166000 seconds]
[Time delta from previous displayed frame: 0.032478000 seconds]
[Time since reference or first frame: 4.661311000 seconds]

Frame Number: 1476
Frame Length: 95 bytes (760 bits)
Capture Length: 95 bytes (760 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 75

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 73
Identification: 0x627c (25212)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc797 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 53192, Dst Port: 53
Source Port: 53192
Destination Port: 53
Length: 53
Checksum: 0x4a62 [unverified]
[Checksum Status: Unverified]
[Stream index: 47]
Domain Name System (query)
Transaction ID: 0xc9f7
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... .0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.enterprise.localist.com: type AAAA, class IN
Name: mit.enterprise.localist.com
[Name Length: 27]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1519]
No. Time Source Destination Protocol Length Info
1498 2018-10-17 16:36:35.234034 202.117.112.3 10.173.88.157 DNS 149 Standard query response
0xc9f7 AAAA mit.enterprise.localist.com SOA dns1.easydns.com
Frame 1498: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.234034000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.234034000 seconds
[Time delta from previous captured frame: 0.218911000 seconds]
[Time delta from previous displayed frame: 0.329256000 seconds]
[Time since reference or first frame: 4.990567000 seconds]
Frame Number: 1498
Frame Length: 149 bytes (1192 bits)
Capture Length: 149 bytes (1192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 129
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 127
Identification: 0x520b (21003)
Flags: 0x0000
0... = Reserved bit: Not set

.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8ea0 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 53192
Source Port: 53
Destination Port: 53192
Length: 107
Checksum: 0xf725 [unverified]
[Checksum Status: Unverified]
[Stream index: 46]

Domain Name System (response)
Transaction ID: 0xc9f7
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
.... 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
mit.enterprise.localist.com: type AAAA, class IN
Name: mit.enterprise.localist.com
[Name Length: 27]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
localist.com: type SOA, class IN, mname dns1.easydns.com
Name: localist.com
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 1200
Data length: 42
Primary name server: dns1.easydns.com
Responsible authority's mailbox: zone.easydns.com
Serial Number: 1407529449
Refresh Interval: 21600 (6 hours)
Retry Interval: 7200 (2 hours)
Expire limit: 604800 (7 days)
Minimum TTL: 1200 (20 minutes)
[Request In: 1429]
[Time: 0.361734000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1499	2018-10-17 16:36:35.235933	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xe150

A connect.mit.edu
Frame 1499: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.235933000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.235933000 seconds
[Time delta from previous captured frame: 0.001899000 seconds]
[Time delta from previous displayed frame: 0.001899000 seconds]
[Time since reference or first frame: 4.992466000 seconds]
Frame Number: 1499
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37e7 (14311)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa506 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 65167, Dst Port: 53
Source Port: 65167
Destination Port: 53
Length: 41
Checksum: 0x615b [unverified]
[Checksum Status: Unverified]
[Stream index: 48]
Domain Name System (query)
Transaction ID: 0xe150
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type A, class IN
Name: connect.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1501]
No. Time Source Destination Protocol Length Info
1500 2018-10-17 16:36:35.265065 10.173.88.157 218.30.19.40 DNS 83 Standard query 0xe150
A connect.mit.edu
Frame 1500: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.265065000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.265065000 seconds
[Time delta from previous captured frame: 0.029132000 seconds]
[Time delta from previous displayed frame: 0.029132000 seconds]

[Time since reference or first frame: 5.021598000 seconds]
Frame Number: 1500
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 61
Identification: 0x627d (25213)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 65167, Dst Port: 53
Source Port: 65167
Destination Port: 53
Length: 41
Checksum: 0xae8d [unverified]
[Checksum Status: Unverified]
[Stream index: 49]

Domain Name System (query)
Transaction ID: 0xe150
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... 0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... 0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type A, class IN
Name: connect.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1505]

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

1501 2018-10-17 16:36:35.291138 202.117.112.3 10.173.88.157 DNS 322 Standard query response
0xe150 A connect.mit.edu A 18.9.22.85 NS k.edu-servers.net NS i.edu-servers.net NS m.edu-servers.net NS g.edu-servers.net NS b.edu-servers.net NS c.edu-servers.net NS e.edu-servers.net NS h.edu-servers.net NS j.edu-servers.net NS a.edu-servers.net NS l.edu-servers.net NS d.edu-servers.net NS f.edu-servers.net
Frame 1501: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.291138000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.291138000 seconds
[Time delta from previous captured frame: 0.026073000 seconds]
[Time delta from previous displayed frame: 0.026073000 seconds]
[Time since reference or first frame: 5.047671000 seconds]
Frame Number: 1501
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 300
Identification: 0x520c (21004)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8df2 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 65167
Source Port: 53
Destination Port: 65167
Length: 280
Checksum: 0xeab4 [unverified]
[Checksum Status: Unverified]
[Stream index: 48]
Domain Name System (response)
Transaction ID: 0xe150
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server

....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

connect.mit.edu: type A, class IN
Name: connect.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

connect.mit.edu: type A, class IN, addr 18.9.22.85
Name: connect.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.22.85

Authoritative nameservers

edu: type NS, class IN, ns k.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 19

Name Server: k.edu-servers.net

edu: type NS, class IN, ns i.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: i.edu-servers.net

edu: type NS, class IN, ns m.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: m.edu-servers.net

edu: type NS, class IN, ns g.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: g.edu-servers.net

edu: type NS, class IN, ns b.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: b.edu-servers.net

edu: type NS, class IN, ns c.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: c.edu-servers.net

edu: type NS, class IN, ns e.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: e.edu-servers.net

edu: type NS, class IN, ns h.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4

Name Server: h.edu-servers.net

Name Server: h.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: a.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: d.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: f.edu-servers.net
[Request In: 1499]
[Time: 0.055205000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1502	2018-10-17 16:36:35.294336	10.173.88.157	202.117.112.3	DNS	83	Standard query 0x2160

A connect.mit.edu
Frame 1502: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.294336000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.294336000 seconds
[Time delta from previous captured frame: 0.003198000 seconds]
[Time delta from previous displayed frame: 0.003198000 seconds]
[Time since reference or first frame: 5.050869000 seconds]
Frame Number: 1502
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x37e8 (14312)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa505 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 62519, Dst Port: 53
Source Port: 62519
Destination Port: 53
Length: 41
Checksum: 0x2ba4 [unverified]
[Checksum Status: Unverified]
[Stream index: 50]
Domain Name System (query)
Transaction ID: 0x2160
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type A, class IN
 Name: connect.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1503]
No. Time Source Destination Protocol Length Info
1503 2018-10-17 16:36:35.295130 202.117.112.3 10.173.88.157 DNS 322 Standard query response
0x2160 A connect.mit.edu A 18.9.22.85 NS b.edu-servers.net NS c.edu-servers.net NS e.edu-servers.net NS g.edu-servers.net NS h.edu-servers.net NS i.edu-servers.net NS l.edu-servers.net NS a.edu-servers.net NS k.edu-servers.net NS j.edu-servers.net NS m.edu-servers.net NS d.edu-servers.net NS f.edu-servers.net
Frame 1503: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.295130000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.295130000 seconds
[Time delta from previous captured frame: 0.000794000 seconds]
[Time delta from previous displayed frame: 0.000794000 seconds]
[Time since reference or first frame: 5.051663000 seconds]
Frame Number: 1503
Frame Length: 322 bytes (2576 bits)
Capture Length: 322 bytes (2576 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 302

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 300
Identification: 0x520d (21005)
Flags: 0x0000

0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8df1 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 62519

Source Port: 53
Destination Port: 62519
Length: 280
Checksum: 0xbdf4 [unverified]
[Checksum Status: Unverified]
[Stream index: 50]

Domain Name System (response)

Transaction ID: 0x2160
Flags: 0x8180 Standard query response, No error

1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0

Queries

connect.mit.edu: type A, class IN
 Name: connect.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

connect.mit.edu: type A, class IN, addr 18.9.22.85
 Name: connect.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.9.22.85

Authoritative nameservers

edu: type NS, class IN, ns b.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 19
 Name Server: b.edu-servers.net

```
edu: type NS, class IN, ns c.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: c.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: e.edu-servers.net
edu: type NS, class IN, ns g.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: g.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: h.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: i.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: l.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: a.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: k.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: j.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: m.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
  Name: edu
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 172718
  Data length: 4
  Name Server: d.edu-servers.net
```

edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: f.edu-servers.net

[Request In: 1502]
[Time: 0.000794000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1504	2018-10-17 16:36:35.298026	10.173.88.157	202.117.112.3	DNS	83	Standard query 0xf5de

AAAA connect.mit.edu

Frame 1504: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.298026000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.298026000 seconds
[Time delta from previous captured frame: 0.002896000 seconds]
[Time delta from previous displayed frame: 0.002896000 seconds]
[Time since reference or first frame: 5.054559000 seconds]
Frame Number: 1504
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 61
Identification: 0x37e9 (14313)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa504 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 61900, Dst Port: 53
Source Port: 61900
Destination Port: 53
Length: 41
Checksum: 0x3e90 [unverified]
[Checksum Status: Unverified]
[Stream index: 51]

Domain Name System (query)
Transaction ID: 0xf5de
Flags: 0x0100 Standard query

0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type AAAA, class IN
 Name: connect.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
[Response In: 1507]

No.	Time	Source	Destination	Protocol	Length	Info
1505	2018-10-17 16:36:35.318313	218.30.19.40	10.173.88.157	DNS	99	Standard query response

Frame 1505: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.318313000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.318313000 seconds
[Time delta from previous captured frame: 0.020287000 seconds]
[Time delta from previous displayed frame: 0.020287000 seconds]
[Time since reference or first frame: 5.074846000 seconds]
Frame Number: 1505
Frame Length: 99 bytes (792 bits)
Capture Length: 99 bytes (792 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 79
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 77
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1... = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf10f [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 65167

Source Port: 53
Destination Port: 65167
Length: 57
Checksum: 0xb4fc [unverified]
[Checksum Status: Unverified]
[Stream index: 49]
Domain Name System (response)
Transaction ID: 0xe150
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.0... = Authoritative: Server is not an authority for domain
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
.0... = Z: reserved (0)
.0. = Answer authenticated: Answer/authority portion was not authenticated by the server
.0 = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type A, class IN
 Name: connect.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
connect.mit.edu: type A, class IN, addr 18.9.22.85
 Name: connect.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.9.22.85
[Request In: 1500]
[Time: 0.053248000 seconds]
No. Time Source Destination Protocol Length Info
1506 2018-10-17 16:36:35.325020 10.173.88.157 218.30.19.40 DNS 83 Standard query 0xf5de
AAAA connect.mit.edu
Frame 1506: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.325020000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.325020000 seconds
[Time delta from previous captured frame: 0.006707000 seconds]
[Time delta from previous displayed frame: 0.006707000 seconds]
[Time since reference or first frame: 5.081553000 seconds]
Frame Number: 1506
Frame Length: 83 bytes (664 bits)
Capture Length: 83 bytes (664 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 63

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 61
Identification: 0x627e (25214)
Flags: 0x0000
0.... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc7a1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 61900, Dst Port: 53
Source Port: 61900
Destination Port: 53
Length: 41
Checksum: 0x8bc2 [unverified]
[Checksum Status: Unverified]
[Stream index: 52]
Domain Name System (query)
Transaction ID: 0xf5de
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
connect.mit.edu: type AAAA, class IN
Name: connect.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1509]
No. Time Source Destination Protocol Length Info
1507 2018-10-17 16:36:35.352841 202.117.112.3 10.173.88.157 DNS 148 Standard query response
0xf5de AAAA connect.mit.edu use2.akam.net
Frame 1507: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.352841000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.352841000 seconds
[Time delta from previous captured frame: 0.027821000 seconds]
[Time delta from previous displayed frame: 0.027821000 seconds]
[Time since reference or first frame: 5.109374000 seconds]
Frame Number: 1507
Frame Length: 148 bytes (1184 bits)
Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0 = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 128

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 126

Identification: 0x520e (21006)

Flags: 0x0000

0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8e9e [validation disabled]
[Header checksum status: Unverified]

Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 61900

Source Port: 53
Destination Port: 61900
Length: 106

Checksum: 0x84a0 [unverified]
[Checksum Status: Unverified]
[Stream index: 51]

Domain Name System (response)

Transaction ID: 0xf5de

Flags: 0x8180 Standard query response, No error

1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 0

Queries

connect.mit.edu: type AAAA, class IN

Name: connect.mit.edu
[Name Length: 15]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers

mit.edu: type SOA, class IN, mname use2.akam.net

Name: mit.edu
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 900
Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)

[Request In: 1504]
[Time: 0.054815000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1508	2018-10-17 16:36:35.354118	10.173.88.157	202.117.112.3	DNS	85	Standard query 0xd5b4
A mitadmissions.org						
Frame 1508: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0						
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})						
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 17, 2018 16:36:35.354118000 中国标准时间						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1539765395.354118000 seconds						
[Time delta from previous captured frame: 0.001277000 seconds]						
[Time delta from previous displayed frame: 0.001277000 seconds]						
[Time since reference or first frame: 5.110651000 seconds]						
Frame Number: 1508						
Frame Length: 85 bytes (680 bits)						
Capture Length: 85 bytes (680 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]						
[Coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
.... .0. = LG bit: Globally unique address (factory default)						
.... ..0. = IG bit: Individual address (unicast)						
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
.... .0. = LG bit: Globally unique address (factory default)						
.... ..0. = IG bit: Individual address (unicast)						
Type: PPPoE Session (0x8864)						
PPP-over-Ethernet Session						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Session Data (0x00)						
Session ID: 0x629d						
Payload Length: 65						
Point-to-Point Protocol						
Protocol: Internet Protocol version 4 (0x0021)						
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
0000 00.. = Differentiated Services Codepoint: Default (0)						
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
Total Length: 63						
Identification: 0x37ea (14314)						
Flags: 0x0000						
0... = Reserved bit: Not set						
.0.. = Don't fragment: Not set						
..0. = More fragments: Not set						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0xa501 [validation disabled]						
[Header checksum status: Unverified]						
Source: 10.173.88.157						
Destination: 202.117.112.3						
User Datagram Protocol, Src Port: 49739, Dst Port: 53						
Source Port: 49739						
Destination Port: 53						
Length: 43						
Checksum: 0xbfc2 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 53]						
Domain Name System (query)						
Transaction ID: 0xd5b4						
Flags: 0x0100 Standard query						
0... = Response: Message is a query						
.000 0... = Opcode: Standard query (0)						
.... ..0. = Truncated: Message is not truncated						
.... ...1 = Recursion desired: Do query recursively						
....0. = Z: reserved (0)						
....0 = Non-authenticated data: Unacceptable						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						

Additional RRs: 0
Queries
mitadmissions.org: type A, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1511]

No.	Time	Source	Destination	Protocol	Length	Info
1509	2018-10-17 16:36:35.379998	218.30.19.40	10.173.88.157	DNS	148	Standard query response

0xf5de AAAA connect.mit.edu SOA use2.akam.net
Frame 1509: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.379998000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.379998000 seconds
[Time delta from previous captured frame: 0.025880000 seconds]
[Time delta from previous displayed frame: 0.025880000 seconds]
[Time since reference or first frame: 5.136531000 seconds]
Frame Number: 1509
Frame Length: 148 bytes (1184 bits)
Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 128
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 126
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0.... = Reserved bit: Not set
.1.... = Don't fragment: Set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0de [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61900
Source Port: 53
Destination Port: 61900
Length: 106
Checksum: 0x4dcf [unverified]
[Checksum Status: Unverified]
[Stream index: 52]
Domain Name System (response)
Transaction ID: 0xf5de
Flags: 0x8180 Standard query response, No error

1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
connect.mit.edu: type AAAA, class IN
 Name: connect.mit.edu
 [Name Length: 15]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)

Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)
 [Request In: 1506]
 [Time: 0.054978000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1510	2018-10-17 16:36:35.380312	10.173.88.157	218.30.19.40	DNS	85	Standard query 0xd5b4

A mitadmissions.org
Frame 1510: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:35.380312000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765395.380312000 seconds
 [Time delta from previous captured frame: 0.000314000 seconds]
 [Time delta from previous displayed frame: 0.000314000 seconds]
 [Time since reference or first frame: 5.136845000 seconds]
 Frame Number: 1510
 Frame Length: 85 bytes (680 bits)
 Capture Length: 85 bytes (680 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0.... = LG bit: Globally unique address (factory default)
 0.... = IG bit: Individual address (unicast)
 Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0.... = LG bit: Globally unique address (factory default)
 0.... = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 65

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x627f (25215)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79e [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 49739, Dst Port: 53
Source Port: 49739
Destination Port: 53
Length: 43
Checksum: 0x0cf5 [unverified]
[Checksum Status: Unverified]
[Stream index: 54]
Domain Name System (query)
Transaction ID: 0xd5b4
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0.. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mitadmissions.org: type A, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1525]
No. Time Source Destination Protocol Length Info
1511 2018-10-17 16:36:35.516965 202.117.112.3 10.173.88.157 DNS 255 Standard query response
0xd5b4 A mitadmissions.org A 104.24.22.109 A 104.24.21.109 NS a2.org.afiliias-nst.info NS b0.org.afiliias-nst.org NS
b2.org.afiliias-nst.org NS c0.org.afiliias-nst.info NS a0.org.afiliias-nst.info NS d0.org.afiliias-nst.org
Frame 1511: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.516965000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.516965000 seconds
[Time delta from previous captured frame: 0.136653000 seconds]
[Time delta from previous displayed frame: 0.136653000 seconds]
[Time since reference or first frame: 5.273498000 seconds]
Frame Number: 1511
Frame Length: 255 bytes (2040 bits)
Capture Length: 255 bytes (2040 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.0. = LG bit: Globally unique address (factory default)
.0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.0. = LG bit: Globally unique address (factory default)
.0 = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 235
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 233
Identification: 0x520f (21007)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e32 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 49739
Source Port: 53
Destination Port: 49739
Length: 213
Checksum: 0xb0ca [unverified]
[Checksum Status: Unverified]
[Stream index: 53]
Domain Name System (response)
Transaction ID: 0xd5b4
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 0
Queries
mitadmissions.org: type A, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
mitadmissions.org: type A, class IN, addr 104.24.22.109
Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.24.22.109
mitadmissions.org: type A, class IN, addr 104.24.21.109
Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.24.21.109
Authoritative nameservers
org: type NS, class IN, ns a2.org.afilias-nst.info
Name: org

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 25
Name Server: a2.org.afilias-nst.info
org: type NS, class IN, ns b0.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 21
Name Server: b0.org.afilias-nst.org
org: type NS, class IN, ns b2.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: b2.org.afilias-nst.org
org: type NS, class IN, ns c0.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: c0.org.afilias-nst.info
org: type NS, class IN, ns a0.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: a0.org.afilias-nst.info
org: type NS, class IN, ns d0.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: d0.org.afilias-nst.org
[Request In: 1508]
[Time: 0.162847000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1512	2018-10-17 16:36:35.521287	10.173.88.157	202.117.112.3	DNS	85	Standard query 0x50db

A mitadmissions.org
Frame 1512: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.521287000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.521287000 seconds
[Time delta from previous captured frame: 0.004322000 seconds]
[Time delta from previous displayed frame: 0.004322000 seconds]
[Time since reference or first frame: 5.277820000 seconds]
Frame Number: 1512
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)

Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37eb (14315)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa500 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 54767, Dst Port: 53
Source Port: 54767
Destination Port: 53
Length: 43
Checksum: 0x30f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 55]
Domain Name System (query)
Transaction ID: 0x50db
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mitadmissions.org: type A, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1513]
No. Time Source Destination Protocol Length Info
1513 2018-10-17 16:36:35.522122 202.117.112.3 10.173.88.157 DNS 255 Standard query response
0x50db A mitadmissions.org A 104.24.21.109 A 104.24.22.109 NS c0.org.afiliias-nst.info NS d0.org.afiliias-nst.org NS
b0.org.afiliias-nst.org NS a2.org.afiliias-nst.info NS b2.org.afiliias-nst.org NS a0.org.afiliias-nst.info
Frame 1513: 255 bytes on wire (2040 bits), 255 bytes captured (2040 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.522122000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.522122000 seconds
[Time delta from previous captured frame: 0.000835000 seconds]
[Time delta from previous displayed frame: 0.000835000 seconds]
[Time since reference or first frame: 5.278655000 seconds]
Frame Number: 1513
Frame Length: 255 bytes (2040 bits)
Capture Length: 255 bytes (2040 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 235
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 233
Identification: 0x5210 (21008)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e31 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 54767
Source Port: 53
Destination Port: 54767
Length: 213
Checksum: 0x41e0 [unverified]
[Checksum Status: Unverified]
[Stream index: 55]
Domain Name System (response)
Transaction ID: 0x50db
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 0
Queries
mitadmissions.org: type A, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
mitadmissions.org: type A, class IN, addr 104.24.21.109
Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.24.21.109
mitadmissions.org: type A, class IN, addr 104.24.22.109
Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300

Data length: 4
Address: 104.24.22.109

Authoritative nameservers

org: type NS, class IN, ns c0.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 25
Name Server: c0.org.afilias-nst.info

org: type NS, class IN, ns d0.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 21
Name Server: d0.org.afilias-nst.org

org: type NS, class IN, ns b0.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: b0.org.afilias-nst.org

org: type NS, class IN, ns a2.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: a2.org.afilias-nst.info

org: type NS, class IN, ns b2.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: b2.org.afilias-nst.org

org: type NS, class IN, ns a0.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169197
Data length: 5
Name Server: a0.org.afilias-nst.info

[Request In: 1512]
[Time: 0.000835000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1514	2018-10-17 16:36:35.523199	10.173.88.157	202.117.112.3	DNS	85	Standard query 0x8e27

AAAA mitadmissions.org

Frame 1514: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:35.523199000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765395.523199000 seconds

[Time delta from previous captured frame: 0.001077000 seconds]

[Time delta from previous displayed frame: 0.001077000 seconds]

[Time since reference or first frame: 5.279732000 seconds]

Frame Number: 1514

Frame Length: 85 bytes (680 bits)

Capture Length: 85 bytes (680 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
 PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 65
 Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 63
 Identification: 0x37ec (14316)
 Flags: 0x0000
 0.... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa4ff [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.173.88.157
 Destination: 202.117.112.3
 User Datagram Protocol, Src Port: 59315, Dst Port: 53
 Source Port: 59315
 Destination Port: 53
 Length: 43
 Checksum: 0xc6e7 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 56]
 Domain Name System (query)
 Transaction ID: 0x8e27
 Flags: 0x0100 Standard query
 0.... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0... = Z: reserved (0)
0 = Non-authenticated data: Unacceptable
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 mitadmissions.org: type AAAA, class IN
 Name: mitadmissions.org
 [Name Length: 17]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1531]

No.	Time	Source	Destination	Protocol	Length	Info
1515	2018-10-17 16:36:35.541405	10.173.88.157	218.30.19.40	DNS	85	Standard query 0x8e27

 AAAA mitadmissions.org
 Frame 1515: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:35.541405000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765395.541405000 seconds
 [Time delta from previous captured frame: 0.018206000 seconds]
 [Time delta from previous displayed frame: 0.018206000 seconds]
 [Time since reference or first frame: 5.297938000 seconds]
 Frame Number: 1515
 Frame Length: 85 bytes (680 bits)
 Capture Length: 85 bytes (680 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x6280 (25216)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79d [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 59315, Dst Port: 53
Source Port: 59315
Destination Port: 53
Length: 43
Checksum: 0x141a [unverified]
[Checksum Status: Unverified]
[Stream index: 57]
Domain Name System (query)
Transaction ID: 0x8e27
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mitadmissions.org: type AAAA, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1549]
No. Time Source Destination Protocol Length Info
1516 2018-10-17 16:36:35.631009 202.117.112.3 10.173.88.157 DNS 335 Standard query response
0x1609 A mit.enterprise.localist.com A 199.19.67.172 NS a.gtld-servers.net NS g.gtld-servers.net NS l.gtld-servers.net NS k.gtld-servers.net NS e.gtld-servers.net NS h.gtld-servers.net NS d.gtld-servers.net NS b.gtld-servers.net NS j.gtld-servers.net NS f.gtld-servers.net NS i.gtld-servers.net NS c.gtld-servers.net NS m.gtld-servers.net
Frame 1516: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.631009000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.631009000 seconds

[Time delta from previous captured frame: 0.089604000 seconds]
[Time delta from previous displayed frame: 0.089604000 seconds]
[Time since reference or first frame: 5.387542000 seconds]
Frame Number: 1516
Frame Length: 335 bytes (2680 bits)
Capture Length: 335 bytes (2680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0 = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0 = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 315
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 313
Identification: 0x5211 (21009)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de0 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 63833
Source Port: 53
Destination Port: 63833
Length: 293
Checksum: 0x8662 [unverified]
[Checksum Status: Unverified]
[Stream index: 44]
Domain Name System (response)
 Transaction ID: 0x1609
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0.. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0.. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0 = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
 mit.enterprise.localist.com: type A, class IN
 Name: mit.enterprise.localist.com
 [Name Length: 27]
 [Label Count: 4]

Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

mit.enterprise.localist.com: type A, class IN, addr 199.19.67.172

Name: mit.enterprise.localist.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 1200

Data length: 4

Address: 199.19.67.172

Authoritative nameservers

com: type NS, class IN, ns a.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 20

Name Server: a.gtld-servers.net

com: type NS, class IN, ns g.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: g.gtld-servers.net

com: type NS, class IN, ns l.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: l.gtld-servers.net

com: type NS, class IN, ns k.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: k.gtld-servers.net

com: type NS, class IN, ns e.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: e.gtld-servers.net

com: type NS, class IN, ns h.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: h.gtld-servers.net

com: type NS, class IN, ns d.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: d.gtld-servers.net

com: type NS, class IN, ns b.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: b.gtld-servers.net

com: type NS, class IN, ns j.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169180

Data length: 4

Name Server: j.gtld-servers.net

com: type NS, class IN, ns f.gtld-servers.net

Name: com

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)
Time to live: 169180
Data length: 4
Name Server: f.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169180
Data length: 4
Name Server: i.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169180
Data length: 4
Name Server: c.gtld-servers.net
com: type NS, class IN, ns m.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169180
Data length: 4
Name Server: m.gtld-servers.net
[Request In: 1367]
[Time: 0.795912000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1517	2018-10-17 16:36:35.631010	202.117.112.3	10.173.88.157	DNS	365	Standard query response

0x1494 A calendar.mit.edu CNAME mit.enterprise.localist.com A 199.19.67.172 NS d.gtld-servers.net NS a.gtld-servers.net NS h.gtld-servers.net NS e.gtld-servers.net NS l.gtld-servers.net NS b.gtld-servers.net NS g.gtld-servers.net NS j.gtld-servers.net NS i.gtld-servers.net NS f.gtld-servers.net NS k.gtld-servers.net NS c.gtld-servers.net NS m.gtld-servers.net
Frame 1517: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.631010000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.631010000 seconds
[Time delta from previous captured frame: 0.000001000 seconds]
[Time delta from previous displayed frame: 0.000001000 seconds]
[Time since reference or first frame: 5.387543000 seconds]
Frame Number: 1517
Frame Length: 365 bytes (2920 bits)
Capture Length: 365 bytes (2920 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 345
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 343
Identification: 0x5212 (21010)
Flags: 0x0000

0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dc1 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 57780
Source Port: 53
Destination Port: 57780
Length: 323
Checksum: 0x348e [unverified]
[Checksum Status: Unverified]
[Stream index: 24]

Domain Name System (response)
Transaction ID: 0x1494
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 2
Authority RRs: 13
Additional RRs: 0

Queries
calendar.mit.edu: type A, class IN
 Name: calendar.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers
calendar.mit.edu: type CNAME, class IN, cname mit.enterprise.localist.com
 Name: calendar.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 29
 CNAME: mit.enterprise.localist.com
mit.enterprise.localist.com: type A, class IN, addr 199.19.67.172
 Name: mit.enterprise.localist.com
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1200
 Data length: 4
 Address: 199.19.67.172

Authoritative nameservers
com: type NS, class IN, ns d.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169180
 Data length: 20
 Name Server: d.gtld-servers.net
com: type NS, class IN, ns a.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169180
 Data length: 4
 Name Server: a.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169180
 Data length: 4

```

Name Server: h.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: e.gtld-servers.net
com: type NS, class IN, ns l.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: l.gtld-servers.net
com: type NS, class IN, ns b.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: b.gtld-servers.net
com: type NS, class IN, ns g.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: g.gtld-servers.net
com: type NS, class IN, ns j.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: j.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: i.gtld-servers.net
com: type NS, class IN, ns f.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: f.gtld-servers.net
com: type NS, class IN, ns k.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: k.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: c.gtld-servers.net
com: type NS, class IN, ns m.gtld-servers.net
  Name: com
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169180
  Data length: 4
  Name Server: m.gtld-servers.net

```

[Request In: 936]

[Time: 2.079880000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1518	2018-10-17 16:36:35.664663	10.173.88.157	202.117.112.3	DNS	79	Standard query 0xffe8

AAAA twitter.com

Frame 1518: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.664663000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.664663000 seconds
[Time delta from previous captured frame: 0.033653000 seconds]
[Time delta from previous displayed frame: 0.033653000 seconds]
[Time since reference or first frame: 5.421196000 seconds]
Frame Number: 1518
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x000)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37ed (14317)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa504 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 61277, Dst Port: 53
Source Port: 61277
Destination Port: 53
Length: 37
Checksum: 0x88cf [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
Domain Name System (query)
Transaction ID: 0xffe8
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 911]
[DNS query retransmission. Original request in frame 911]
[Severity level: Warning]
[Group: Protocol]
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0

Additional RRs: 0
Queries
 twitter.com: type AAAA, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
[Retransmitted request. Original request in: 911]
[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
1519	2018-10-17 16:36:35.773261	218.30.19.40	10.173.88.157	DNS	149	Standard query response

0xc9f7 AAAA mit.enterprise.localist.com SOA dns1.easydns.com
Frame 1519: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:35.773261000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765395.773261000 seconds
[Time delta from previous captured frame: 0.108598000 seconds]
[Time delta from previous displayed frame: 0.108598000 seconds]
[Time since reference or first frame: 5.529794000 seconds]
Frame Number: 1519
Frame Length: 149 bytes (1192 bits)
Capture Length: 149 bytes (1192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 129
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 127
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0dd [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 53192
Source Port: 53
Destination Port: 53192
Length: 107
Checksum: 0x7059 [unverified]
[Checksum Status: Unverified]
[Stream index: 47]
Domain Name System (response)
Transaction ID: 0xc9f7

Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
mit.enterprise.localist.com: type AAAA, class IN
Name: mit.enterprise.localist.com
[Name Length: 27]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
localist.com: type SOA, class IN, mname dns1.easydns.com
Name: localist.com
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 900
Data length: 42
Primary name server: dns1.easydns.com
Responsible authority's mailbox: zone.easydns.com
Serial Number: 1407529449
Refresh Interval: 21600 (6 hours)
Retry Interval: 7200 (2 hours)
Expire limit: 604800 (7 days)
Minimum TTL: 1200 (20 minutes)

[Request In: 1476]
[Time: 0.868483000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1522	2018-10-17 16:36:36.008167	202.117.112.3	10.173.88.157	DNS	79	Standard query response

0xffe8 Server failure AAAA twitter.com
Frame 1522: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.008167000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.008167000 seconds
[Time delta from previous captured frame: 0.031461000 seconds]
[Time delta from previous displayed frame: 0.234906000 seconds]
[Time since reference or first frame: 5.764700000 seconds]
Frame Number: 1522
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0.... = LG bit: Globally unique address (factory default)
.... ..0.... = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0.... = LG bit: Globally unique address (factory default)
.... ..0.... = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x5213 (21011)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8ede [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 61277
Source Port: 53
Destination Port: 61277
Length: 37
Checksum: 0x084d [unverified]
[Checksum Status: Unverified]
[Stream index: 11]
Domain Name System (response)
Transaction ID: 0xffe8
Flags: 0x8182 Standard query response, Server failure
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0. = Non-authenticated data: Unacceptable
.... 0010 = Reply code: Server failure (2)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 twitter.com: type AAAA, class IN
 Name: twitter.com
 [Name Length: 11]
 [Label Count: 2]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Request In: 911]
 [Time: 2.576737000 seconds]
No. Time Source Destination Protocol Length Info
1523 2018-10-17 16:36:36.009453 10.173.88.157 202.117.112.3 DNS 85 Standard query 0xa4da
A libraries.mit.edu
Frame 1523: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.009453000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.009453000 seconds
[Time delta from previous captured frame: 0.001286000 seconds]
[Time delta from previous displayed frame: 0.001286000 seconds]
[Time since reference or first frame: 5.765986000 seconds]
Frame Number: 1523
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37ee (14318)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
.... 0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fd [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 63115, Dst Port: 53
Source Port: 63115
Destination Port: 53
Length: 43
Checksum: 0x3170 [unverified]
[Checksum Status: Unverified]
[Stream index: 58]
Domain Name System (query)
Transaction ID: 0xa4da
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 libraries.mit.edu: type A, class IN
 Name: libraries.mit.edu
 [Name Length: 17]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1526]
No. Time Source Destination Protocol Length Info
1524 2018-10-17 16:36:36.045067 10.173.88.157 218.30.19.40 DNS 85 Standard query 0xa4da
A libraries.mit.edu
Frame 1524: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.045067000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.045067000 seconds
[Time delta from previous captured frame: 0.035614000 seconds]
[Time delta from previous displayed frame: 0.035614000 seconds]
[Time since reference or first frame: 5.801600000 seconds]
Frame Number: 1524
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)

[Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 65

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 63
 Identification: 0x6281 (25217)
 Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xc79c [validation disabled]
 [Header checksum status: Unverified]

Source: 10.173.88.157
 Destination: 218.30.19.40

User Datagram Protocol, Src Port: 63115, Dst Port: 53
 Source Port: 63115
 Destination Port: 53
 Length: 43
 Checksum: 0x7ea2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 59]

Domain Name System (query)
 Transaction ID: 0xa4da
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0.. = Z: reserved (0)
0 = Non-authenticated data: Unacceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0

Queries
 libraries.mit.edu: type A, class IN
 Name: libraries.mit.edu
 [Name Length: 17]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1530]

No.	Time	Source	Destination	Protocol	Length	Info
1525	2018-10-17 16:36:36.091624	218.30.19.40	10.173.88.157	DNS	117	Standard query response

0xd5b4 A mitadmissions.org A 104.24.22.109 A 104.24.21.109
 Frame 1525: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.091624000 中国标准时间
[Time shift for this packet: 0.00000000 seconds]
Epoch Time: 1539765396.091624000 seconds
[Time delta from previous captured frame: 0.046557000 seconds]
[Time delta from previous displayed frame: 0.046557000 seconds]
[Time since reference or first frame: 5.848157000 seconds]
Frame Number: 1525
Frame Length: 117 bytes (936 bits)
Capture Length: 117 bytes (936 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 97
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 95
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0fd [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 49739
Source Port: 53
Destination Port: 49739
Length: 75
Checksum: 0x03b4 [unverified]
[Checksum Status: Unverified]
[Stream index: 54]
Domain Name System (response)
Transaction ID: 0xd5b4
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0. = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
mitadmissions.org: type A, class IN

Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

mitadmissions.org: type A, class IN, addr 104.24.22.109

Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.24.22.109

mitadmissions.org: type A, class IN, addr 104.24.21.109

Name: mitadmissions.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.24.21.109

[Request In: 1510]

[Time: 0.711312000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1526	2018-10-17 16:36:36.169673	202.117.112.3	10.173.88.157	DNS	347	Standard query response

0xa4da A libraries.mit.edu CNAME malgosia.mit.edu A 18.9.49.46 NS g.edu-servers.net NS h.edu-servers.net NS c.edu-servers.net NS j.edu-servers.net NS f.edu-servers.net NS l.edu-servers.net NS i.edu-servers.net NS a.edu-servers.net NS k.edu-servers.net NS d.edu-servers.net NS b.edu-servers.net NS m.edu-servers.net NS e.edu-servers.net

Frame 1526: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.169673000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.169673000 seconds

[Time delta from previous captured frame: 0.078049000 seconds]

[Time delta from previous displayed frame: 0.078049000 seconds]

[Time since reference or first frame: 5.926206000 seconds]

Frame Number: 1526

Frame Length: 347 bytes (2776 bits)

Capture Length: 347 bytes (2776 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 327

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 325

Identification: 0x5214 (21012)

Flags: 0x0000

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)
Header checksum: 0x8dd1 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 63115
Source Port: 53
Destination Port: 63115
Length: 305
Checksum: 0x7961 [unverified]
[Checksum Status: Unverified]
[Stream index: 58]
Domain Name System (response)
Transaction ID: 0xa4da
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 13
Additional RRs: 0
Queries
 libraries.mit.edu: type A, class IN
 Name: libraries.mit.edu
 [Name Length: 17]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
 libraries.mit.edu: type CNAME, class IN, cname malgosia.mit.edu
 Name: libraries.mit.edu
 Type: CNAME (Canonical NAME for an alias) (5)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 11
 CNAME: malgosia.mit.edu
 malgosia.mit.edu: type A, class IN, addr 18.9.49.46
 Name: malgosia.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 4
 Address: 18.9.49.46
Authoritative nameservers
 edu: type NS, class IN, ns g.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 19
 Name Server: g.edu-servers.net
 edu: type NS, class IN, ns h.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: h.edu-servers.net
 edu: type NS, class IN, ns c.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: c.edu-servers.net
 edu: type NS, class IN, ns j.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)

Time to live: 172718
 Data length: 4
 Name Server: j.edu-servers.net
 edu: type NS, class IN, ns f.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: f.edu-servers.net
 edu: type NS, class IN, ns l.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: l.edu-servers.net
 edu: type NS, class IN, ns i.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: i.edu-servers.net
 edu: type NS, class IN, ns a.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: a.edu-servers.net
 edu: type NS, class IN, ns k.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: k.edu-servers.net
 edu: type NS, class IN, ns d.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: d.edu-servers.net
 edu: type NS, class IN, ns b.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: b.edu-servers.net
 edu: type NS, class IN, ns m.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: m.edu-servers.net
 edu: type NS, class IN, ns e.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172718
 Data length: 4
 Name Server: e.edu-servers.net

[Request In: 1523]
 [Time: 0.16022000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1527	2018-10-17 16:36:36.170916	10.173.88.157	202.117.112.3	DNS	84	Standard query 0xfa3c

A malgosia.mit.edu

Frame 1527: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.170916000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.170916000 seconds
[Time delta from previous captured frame: 0.001243000 seconds]
[Time delta from previous displayed frame: 0.001243000 seconds]
[Time since reference or first frame: 5.927449000 seconds]
Frame Number: 1527
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37ef (14319)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fd [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 65429, Dst Port: 53
Source Port: 65429
Destination Port: 53
Length: 42
Checksum: 0x0545 [unverified]
[Checksum Status: Unverified]
[Stream index: 60]
Domain Name System (query)
Transaction ID: 0xfa3c
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
malgosia.mit.edu: type A, class IN
Name: malgosia.mit.edu
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1528]

No.	Time	Source	Destination	Protocol	Length	Info
1528	2018-10-17 16:36:36.172076	202.117.112.3	10.173.88.157	DNS	323	Standard query response
0xfa3c	A malgosia.mit.edu	A 18.9.49.46	NS h.edu-servers.net	NS m.edu-servers.net	NS l.edu-servers.net	NS b.edu-servers.net
NS	j.edu-servers.net	NS i.edu-servers.net	NS d.edu-servers.net	NS f.edu-servers.net	NS e.edu-servers.net	NS a.edu-servers.net
NS	k.edu-servers.net	NS g.edu-servers.net	NS c.edu-servers.net			
Frame 1528: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits) on interface 0						
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})						
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 17, 2018 16:36:36.172076000 中国标准时间						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1539765396.172076000 seconds						
[Time delta from previous captured frame: 0.001160000 seconds]						
[Time delta from previous displayed frame: 0.001160000 seconds]						
[Time since reference or first frame: 5.928609000 seconds]						
Frame Number: 1528						
Frame Length: 323 bytes (2584 bits)						
Capture Length: 323 bytes (2584 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]						
[Coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
.... .0. = LG bit: Globally unique address (factory default)						
.... .0. = IG bit: Individual address (unicast)						
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
.... .0. = LG bit: Globally unique address (factory default)						
.... .0. = IG bit: Individual address (unicast)						
Type: PPPoE Session (0x8864)						
PPP-over-Ethernet Session						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Session Data (0x00)						
Session ID: 0x629d						
Payload Length: 303						
Point-to-Point Protocol						
Protocol: Internet Protocol version 4 (0x0021)						
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
0000 00.. = Differentiated Services Codepoint: Default (0)						
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
Total Length: 301						
Identification: 0x5215 (21013)						
Flags: 0x0000						
0.... = Reserved bit: Not set						
.0.... = Don't fragment: Not set						
..0.... = More fragments: Not set						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 60						
Protocol: UDP (17)						
Header checksum: 0x8de8 [validation disabled]						
[Header checksum status: Unverified]						
Source: 202.117.112.3						
Destination: 10.173.88.157						
User Datagram Protocol, Src Port: 53, Dst Port: 65429						
Source Port: 53						
Destination Port: 65429						
Length: 281						
Checksum: 0x130d [unverified]						
[Checksum Status: Unverified]						
[Stream index: 60]						
Domain Name System (response)						
Transaction ID: 0xfa3c						
Flags: 0x8180 Standard query response, No error						
1.... = Response: Message is a response						
.000 0.... = Opcode: Standard query (0)						
.... .0.. = Authoritative: Server is not an authority for domain						
.... ..0. = Truncated: Message is not truncated						
.... ...1 = Recursion desired: Do query recursively						
.... 1... = Recursion available: Server can do recursive queries						
....0.. = Z: reserved (0)						

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

malgosia.mit.edu: type A, class IN
Name: malgosia.mit.edu
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

malgosia.mit.edu: type A, class IN, addr 18.9.49.46
Name: malgosia.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.49.46

Authoritative nameservers

edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 19
Name Server: h.edu-servers.net

edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: m.edu-servers.net

edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: l.edu-servers.net

edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: b.edu-servers.net

edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: j.edu-servers.net

edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: i.edu-servers.net

edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: d.edu-servers.net

edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718

Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: a.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: k.edu-servers.net
edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: g.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172718
Data length: 4
Name Server: c.edu-servers.net
[Request In: 1527]
[Time: 0.001160000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1529	2018-10-17 16:36:36.173146	10.173.88.157	202.117.112.3	DNS	84	Standard query 0xcdb9

AAAA malgosia.mit.edu
Frame 1529: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.173146000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.173146000 seconds
[Time delta from previous captured frame: 0.001070000 seconds]
[Time delta from previous displayed frame: 0.001070000 seconds]
[Time since reference or first frame: 5.929679000 seconds]
Frame Number: 1529
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64
Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37f0 (14320)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fc [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 59337, Dst Port: 53
Source Port: 59337
Destination Port: 53
Length: 42
Checksum: 0x4979 [unverified]
[Checksum Status: Unverified]
[Stream index: 61]
Domain Name System (query)
Transaction ID: 0xcdb9
Flags: 0x0100 Standard query
 0.... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0... = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 malgosia.mit.edu: type AAAA, class IN
 Name: malgosia.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1536]
No. Time Source Destination Protocol Length Info
1530 2018-10-17 16:36:36.189027 218.30.19.40 10.173.88.157 DNS 124 Standard query response
0xa4da A libraries.mit.edu CNAME malgosia.mit.edu A 18.9.49.46
Frame 1530: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.189027000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.189027000 seconds
[Time delta from previous captured frame: 0.015881000 seconds]
[Time delta from previous displayed frame: 0.015881000 seconds]
[Time since reference or first frame: 5.945560000 seconds]
Frame Number: 1530
Frame Length: 124 bytes (992 bits)
Capture Length: 124 bytes (992 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 104
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 102
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0f6 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 63115
Source Port: 53
Destination Port: 63115
Length: 82
Checksum: 0x5ad9 [unverified]
[Checksum Status: Unverified]
[Stream index: 59]
Domain Name System (response)
Transaction ID: 0xa4da
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
libraries.mit.edu: type A, class IN
Name: libraries.mit.edu
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
libraries.mit.edu: type CNAME, class IN, cname malgosia.mit.edu
Name: libraries.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800
Data length: 11
CNAME: malgosia.mit.edu
malgosia.mit.edu: type A, class IN, addr 18.9.49.46
Name: malgosia.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.49.46
[Request In: 1524]
[Time: 0.143960000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1531	2018-10-17 16:36:36.200572	202.117.112.3	10.173.88.157	DNS	279	Standard query response
0x8e27	AAAA mitadmissions.org AAAA 2606:4700:20::6818:156d	AAAA 2606:4700:20::6818:166d	NS a2.org.afilias-nst.info NS	c0.org.afilias-nst.info NS a0.org.afilias-nst.info NS b0.org.afilias-nst.org NS d0.org.afilias-nst.org NS b2.org.afilias-nst.org		
Frame 1531: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface 0						
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})						
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 17, 2018 16:36:36.200572000 中国标准时间						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1539765396.200572000 seconds						
[Time delta from previous captured frame: 0.011545000 seconds]						
[Time delta from previous displayed frame: 0.011545000 seconds]						
[Time since reference or first frame: 5.957105000 seconds]						
Frame Number: 1531						
Frame Length: 279 bytes (2232 bits)						
Capture Length: 279 bytes (2232 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]						
[Coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)						
.... .0. = LG bit: Globally unique address (factory default)						
.... .0. = IG bit: Individual address (unicast)						
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)						
.... .0. = LG bit: Globally unique address (factory default)						
.... .0. = IG bit: Individual address (unicast)						
Type: PPPoE Session (0x8864)						
PPP-over-Ethernet Session						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Session Data (0x00)						
Session ID: 0x629d						
Payload Length: 259						
Point-to-Point Protocol						
Protocol: Internet Protocol version 4 (0x0021)						
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
0000 00.. = Differentiated Services Codepoint: Default (0)						
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)						
Total Length: 257						
Identification: 0x5216 (21014)						
Flags: 0x0000						
0.... = Reserved bit: Not set						
.0.... = Don't fragment: Not set						
..0.... = More fragments: Not set						
...0 0000 0000 0000 = Fragment offset: 0						
Time to live: 60						
Protocol: UDP (17)						
Header checksum: 0x8e13 [validation disabled]						
[Header checksum status: Unverified]						
Source: 202.117.112.3						
Destination: 10.173.88.157						
User Datagram Protocol, Src Port: 53, Dst Port: 59315						
Source Port: 53						
Destination Port: 59315						
Length: 237						
Checksum: 0xc999 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 56]						
Domain Name System (response)						
Transaction ID: 0x8e27						
Flags: 0x8180 Standard query response, No error						
1.... = Response: Message is a response						
.000 0.... = Opcode: Standard query (0)						
.... .0.. = Authoritative: Server is not an authority for domain						
.... ..0. = Truncated: Message is not truncated						
.... 1.... = Recursion desired: Do query recursively						
.... 1.... = Recursion available: Server can do recursive queries						
....0.. = Z: reserved (0)						

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 2

Authority RRs: 6

Additional RRs: 0

Queries

mitadmissions.org: type AAAA, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Answers

mitadmissions.org: type AAAA, class IN, addr 2606:4700:20::6818:156d

Name: mitadmissions.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16

AAAA Address: 2606:4700:20::6818:156d

mitadmissions.org: type AAAA, class IN, addr 2606:4700:20::6818:166d

Name: mitadmissions.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16

AAAA Address: 2606:4700:20::6818:166d

Authoritative nameservers

org: type NS, class IN, ns a2.org.afiliias-nst.info

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 25

Name Server: a2.org.afiliias-nst.info

org: type NS, class IN, ns c0.org.afiliias-nst.info

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5

Name Server: c0.org.afiliias-nst.info

org: type NS, class IN, ns a0.org.afiliias-nst.info

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5

Name Server: a0.org.afiliias-nst.info

org: type NS, class IN, ns b0.org.afiliias-nst.org

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 21

Name Server: b0.org.afiliias-nst.org

org: type NS, class IN, ns d0.org.afiliias-nst.org

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5

Name Server: d0.org.afiliias-nst.org

org: type NS, class IN, ns b2.org.afiliias-nst.org

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5

Name Server: b2.org.afiliias-nst.org

[Request In: 1514]

[Time: 0.677373000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
A meche.mit.edu	1532 2018-10-17 16:36:36.201832	10.173.88.157	202.117.112.3	DNS	81	Standard query 0xba7f

Frame 1532: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.201832000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.201832000 seconds
[Time delta from previous captured frame: 0.001260000 seconds]
[Time delta from previous displayed frame: 0.001260000 seconds]
[Time since reference or first frame: 5.958365000 seconds]
Frame Number: 1532
Frame Length: 81 bytes (648 bits)
Capture Length: 81 bytes (648 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 61
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 59
Identification: 0x37f1 (14321)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fe [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 52388, Dst Port: 53
Source Port: 52388
Destination Port: 53
Length: 39
Checksum: 0x2f91 [unverified]
[Checksum Status: Unverified]
[Stream index: 62]
Domain Name System (query)
Transaction ID: 0xba7f
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0. = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 meche.mit.edu: type A, class IN

Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1544]

No.	Time	Source	Destination	Protocol	Length	Info
1533	2018-10-17 16:36:36.205081	10.173.88.157	218.30.19.40	DNS	84	Standard query 0xcdb9

AAAA malgosia.mit.edu
Frame 1533: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.205081000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.205081000 seconds
[Time delta from previous captured frame: 0.003249000 seconds]
[Time delta from previous displayed frame: 0.003249000 seconds]
[Time since reference or first frame: 5.961614000 seconds]
Frame Number: 1533
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSVP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x6282 (25218)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79c [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 59337, Dst Port: 53
Source Port: 59337
Destination Port: 53
Length: 42
Checksum: 0x96ab [unverified]
[Checksum Status: Unverified]
[Stream index: 63]
Domain Name System (query)
Transaction ID: 0xcdb9
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated

.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
malgosia.mit.edu: type AAAA, class IN
Name: malgosia.mit.edu
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

[Response In: 1548]

No.	Time	Source	Destination	Protocol	Length	Info
1534	2018-10-17 16:36:36.224742	10.173.88.157	202.117.112.3	DNS	85	Standard query 0xd571

AAAA www.instagram.com
Frame 1534: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.224742000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.224742000 seconds
[Time delta from previous captured frame: 0.019661000 seconds]
[Time delta from previous displayed frame: 0.019661000 seconds]
[Time since reference or first frame: 5.981275000 seconds]
Frame Number: 1534
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ...0. = LG bit: Globally unique address (factory default)
.... ...0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ...0. = LG bit: Globally unique address (factory default)
.... ...0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x37f2 (14322)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4f9 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 64089, Dst Port: 53
Source Port: 64089
Destination Port: 53
Length: 43

Checksum: 0xd0f6 [unverified]
[Checksum Status: Unverified]
[Stream index: 41]

Domain Name System (query)
Transaction ID: 0xd571
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 986]
[DNS query retransmission. Original request in frame 986]
[Severity level: Warning]
[Group: Protocol]

Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type AAAA, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

[Retransmitted request. Original request in: 986]
[Retransmission: True]

No.	Time	Source	Destination	Protocol	Length	Info
1535	2018-10-17 16:36:36.224940	10.173.88.157	218.30.19.40	DNS	81	Standard query 0xba7f

A meche.mit.edu
Frame 1535: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.224940000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.224940000 seconds
[Time delta from previous captured frame: 0.000198000 seconds]
[Time delta from previous displayed frame: 0.000198000 seconds]
[Time since reference or first frame: 5.981473000 seconds]
Frame Number: 1535
Frame Length: 81 bytes (648 bits)
Capture Length: 81 bytes (648 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 61
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 59
Identification: 0x6283 (25219)
Flags: 0x0000

0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79e [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 52388, Dst Port: 53
Source Port: 52388
Destination Port: 53
Length: 39
Checksum: 0x7cc3 [unverified]
[Checksum Status: Unverified]
[Stream index: 64]

Domain Name System (query)
Transaction ID: 0xba7f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
meche.mit.edu: type A, class IN
 Name: meche.mit.edu
 [Name Length: 13]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
[Response In: 1550]

No.	Time	Source	Destination	Protocol	Length	Info
1536	2018-10-17 16:36:36.234996	202.117.112.3	10.173.88.157	DNS	149	Standard query response

0xcd9 AAAA malgosia.mit.edu SOA use2.akam.net

Frame 1536: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.234996000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.234996000 seconds
[Time delta from previous captured frame: 0.010056000 seconds]
[Time delta from previous displayed frame: 0.010056000 seconds]
[Time since reference or first frame: 5.991529000 seconds]
Frame Number: 1536
Frame Length: 149 bytes (1192 bits)
Capture Length: 149 bytes (1192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 129

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 127
Identification: 0x5217 (21015)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e94 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 59337
Source Port: 53
Destination Port: 59337
Length: 107
Checksum: 0xdbb3b [unverified]
[Checksum Status: Unverified]
[Stream index: 61]
Domain Name System (response)
Transaction ID: 0xcdb9
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
malgosia.mit.edu: type AAAA, class IN
Name: malgosia.mit.edu
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
Name: mit.edu
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 900
Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)
[Request In: 1529]
[Time: 0.061850000 seconds]
No. Time Source Destination Protocol Length Info
1537 2018-10-17 16:36:36.238220 10.173.88.157 202.117.112.3 DNS 79 Standard query 0x28c0
A www.edx.org
Frame 1537: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.238220000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.238220000 seconds
[Time delta from previous captured frame: 0.003224000 seconds]

[Time delta from previous displayed frame: 0.003224000 seconds]
[Time since reference or first frame: 5.994753000 seconds]
Frame Number: 1537
Frame Length: 79 bytes (632 bits)
Capture Length: 79 bytes (632 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 59
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 57
Identification: 0x37f3 (14323)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fe [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 58447, Dst Port: 53
Source Port: 58447
Destination Port: 53
Length: 37
Checksum: 0xf8f8 [unverified]
[Checksum Status: Unverified]
[Stream index: 65]
Domain Name System (query)
Transaction ID: 0x28c0
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.edx.org: type A, class IN
Name: www.edx.org
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1538]
No. Time Source Destination Protocol Length Info

1538 2018-10-17 16:36:36.239394 202.117.112.3 10.173.88.157 DNS 360 Standard query response
0x28c0 A www.edx.org CNAME www.edx.org.cdn.cloudflare.net A 117.34.14.192 NS e.gtld-servers.net NS 1.gtld-servers.net NS
b.gtld-servers.net NS i.gtld-servers.net NS f.gtld-servers.net NS d.gtld-servers.net NS j.gtld-servers.net NS h.gtld-
servers.net NS m.gtld-servers.net NS c.gtld-servers.net NS g.gtld-servers.net NS k.gtld-servers.net NS a.gtld-servers.net
Frame 1538: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.239394000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.239394000 seconds
[Time delta from previous captured frame: 0.001174000 seconds]
[Time delta from previous displayed frame: 0.001174000 seconds]
[Time since reference or first frame: 5.995927000 seconds]
Frame Number: 1538
Frame Length: 360 bytes (2880 bits)
Capture Length: 360 bytes (2880 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 340
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 338
Identification: 0x5218 (21016)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dc0 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 58447
Source Port: 53
Destination Port: 58447
Length: 318
Checksum: 0xd440 [unverified]
[Checksum Status: Unverified]
[Stream index: 65]
Domain Name System (response)
Transaction ID: 0x28c0
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server

....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 2

Authority RRs: 13

Additional RRs: 0

Queries

www.edx.org: type A, class IN
Name: www.edx.org
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

www.edx.org: type CNAME, class IN, cname www.edx.org.cdn.cloudflare.net

Name: www.edx.org

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 82

Data length: 32

CNAME: www.edx.org.cdn.cloudflare.net

www.edx.org.cdn.cloudflare.net: type A, class IN, addr 117.34.14.192

Name: www.edx.org.cdn.cloudflare.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 82

Data length: 4

Address: 117.34.14.192

Authoritative nameservers

net: type NS, class IN, ns e.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 17

Name Server: e.gtld-servers.net

net: type NS, class IN, ns l.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

Name Server: l.gtld-servers.net

net: type NS, class IN, ns b.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

Name Server: b.gtld-servers.net

net: type NS, class IN, ns i.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

Name Server: i.gtld-servers.net

net: type NS, class IN, ns f.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

Name Server: f.gtld-servers.net

net: type NS, class IN, ns d.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

Name Server: d.gtld-servers.net

net: type NS, class IN, ns j.gtld-servers.net

Name: net

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 169186

Data length: 4

```
Name Server: j.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: h.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: m.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: c.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: g.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: k.gtld-servers.net
net: type NS, class IN, ns a.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: a.gtld-servers.net
[Request In: 1537]
[Time: 0.001174000 seconds]

No. Time Source Destination Protocol Length Info
1539 2018-10-17 16:36:36.242019 10.173.88.157 202.117.112.3 DNS 98 Standard query 0xeeef2

A www.edx.org.cdn.cloudflare.net
Frame 1539: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
  Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.242019000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.242019000 seconds
[Time delta from previous captured frame: 0.002625000 seconds]
[Time delta from previous displayed frame: 0.002625000 seconds]
[Time since reference or first frame: 5.998552000 seconds]
Frame Number: 1539
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
  Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
    Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0. .... .... .... = IG bit: Individual address (unicast)
  Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
    Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0. .... .... .... = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
```

0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 78
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 76
Identification: 0x37f4 (14324)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4ea [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 49550, Dst Port: 53
Source Port: 49550
Destination Port: 53
Length: 56
Checksum: 0xf40e [unverified]
[Checksum Status: Unverified]
[Stream index: 66]
Domain Name System (query)
Transaction ID: 0xeeef2
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.edx.org.cdn.cloudflare.net: type A, class IN
Name: www.edx.org.cdn.cloudflare.net
[Name Length: 30]
[Label Count: 6]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1540]
No. Time Source Destination Protocol Length Info
1540 2018-10-17 16:36:36.242990 202.117.112.3 10.173.88.157 DNS 335 Standard query response
0xeeef2 A www.edx.org.cdn.cloudflare.net A 117.34.14.192 NS l.gtld-servers.net NS h.gtld-servers.net NS d.gtld-servers.net NS c.gtld-servers.net NS j.gtld-servers.net NS i.gtld-servers.net NS k.gtld-servers.net NS m.gtld-servers.net NS e.gtld-servers.net NS a.gtld-servers.net NS f.gtld-servers.net NS b.gtld-servers.net NS g.gtld-servers.net
Frame 1540: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.242990000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.242990000 seconds
[Time delta from previous captured frame: 0.000971000 seconds]
[Time delta from previous displayed frame: 0.000971000 seconds]
[Time since reference or first frame: 5.999523000 seconds]
Frame Number: 1540
Frame Length: 335 bytes (2680 bits)
Capture Length: 335 bytes (2680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 315
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 313
Identification: 0x5219 (21017)
Flags: 0x0000
0... = Reserved bit: Not set
.0. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dd8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 49550
Source Port: 53
Destination Port: 49550
Length: 293
Checksum: 0xa3b1 [unverified]
[Checksum Status: Unverified]
[Stream index: 66]
Domain Name System (response)
Transaction ID: 0xeeef2
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
www.edx.org.cdn.cloudflare.net: type A, class IN
Name: www.edx.org.cdn.cloudflare.net
[Name Length: 30]
[Label Count: 6]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.edx.org.cdn.cloudflare.net: type A, class IN, addr 117.34.14.192
Name: www.edx.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 82
Data length: 4
Address: 117.34.14.192
Authoritative nameservers

```
net: type NS, class IN, ns l.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 17
  Name Server: l.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: h.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: d.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: c.gtld-servers.net
net: type NS, class IN, ns j.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: j.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: i.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: k.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: m.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: e.gtld-servers.net
net: type NS, class IN, ns a.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: a.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: f.gtld-servers.net
```

net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: b.gtld-servers.net

net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: g.gtld-servers.net

[Request In: 1539]
[Time: 0.000971000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1541	2018-10-17 16:36:36.245586	10.173.88.157	202.117.112.3	DNS	98	Standard query 0xfb84

AAAA www.edx.org.cdn.cloudflare.net

Frame 1541: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.245586000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.245586000 seconds
[Time delta from previous captured frame: 0.002596000 seconds]
[Time delta from previous displayed frame: 0.002596000 seconds]
[Time since reference or first frame: 6.002119000 seconds]
Frame Number: 1541
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 78

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 76
Identification: 0x37f5 (14325)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e9 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 61054, Dst Port: 53
Source Port: 61054
Destination Port: 53

Length: 56
Checksum: 0xba41 [unverified]
[Checksum Status: Unverified]
[Stream index: 67]
Domain Name System (query)
Transaction ID: 0xfbb4
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.edx.org.cdn.cloudflare.net: type AAAA, class IN
Name: www.edx.org.cdn.cloudflare.net
[Name Length: 30]
[Label Count: 6]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1542]
No. Time Source Destination Protocol Length Info
1542 2018-10-17 16:36:36.246732 202.117.112.3 10.173.88.157 DNS 375 Standard query response
0xfbb4 AAAA www.edx.org.cdn.cloudflare.net AAAA 2400:cb00:2048:1::6810:a5e4 AAAA 2400:cb00:2048:1::6810:a4e4 NS a.gtld-servers.net NS e.gtld-servers.net NS k.gtld-servers.net NS m.gtld-servers.net NS c.gtld-servers.net NS i.gtld-servers.net NS g.gtld-servers.net NS b.gtld-servers.net NS f.gtld-servers.net NS j.gtld-servers.net NS d.gtld-servers.net NS h.gtld-servers.net NS l.gtld-servers.net
Frame 1542: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.246732000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.246732000 seconds
[Time delta from previous captured frame: 0.001146000 seconds]
[Time delta from previous displayed frame: 0.001146000 seconds]
[Time since reference or first frame: 6.003265000 seconds]
Frame Number: 1542
Frame Length: 375 bytes (3000 bits)
Capture Length: 375 bytes (3000 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 355
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 353
Identification: 0x521a (21018)
Flags: 0x0000
0... = Reserved bit: Not set

.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8daf [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 61054
Source Port: 53
Destination Port: 61054
Length: 333
Checksum: 0x083a [unverified]
[Checksum Status: Unverified]
[Stream index: 67]

Domain Name System (response)
Transaction ID: 0xfbba4
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 2
Authority RRs: 13
Additional RRs: 0
Queries
www.edx.org.cdn.cloudflare.net: type AAAA, class IN
Name: www.edx.org.cdn.cloudflare.net
[Name Length: 30]
[Label Count: 6]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Answers
www.edx.org.cdn.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2048:1::6810:a5e4
Name: www.edx.org.cdn.cloudflare.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 92
Data length: 16
AAAA Address: 2400:cb00:2048:1::6810:a5e4
www.edx.org.cdn.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2048:1::6810:a4e4
Name: www.edx.org.cdn.cloudflare.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 92
Data length: 16
AAAA Address: 2400:cb00:2048:1::6810:a4e4

Authoritative nameservers
net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 17
Name Server: a.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: k.gtld-servers.net

```

net: type NS, class IN, ns m.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: m.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: c.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: i.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: g.gtld-servers.net
net: type NS, class IN, ns b.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: b.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: f.gtld-servers.net
net: type NS, class IN, ns j.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: j.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: d.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: h.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
  Name: net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169186
  Data length: 4
  Name Server: l.gtld-servers.net
[Request In: 1541]
[Time: 0.001146000 seconds]

```

No.	Time	Source	Destination	Protocol	Length	Info
1543	2018-10-17 16:36:36.249358	10.173.88.157	202.117.112.3	DNS	80	Standard query 0x979f
A	alum.mit.edu					
Frame 1543: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0						
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})						

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.249358000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.249358000 seconds
[Time delta from previous captured frame: 0.002626000 seconds]
[Time delta from previous displayed frame: 0.002626000 seconds]
[Time since reference or first frame: 6.005891000 seconds]
Frame Number: 1543
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 60
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 58
Identification: 0x37f6 (14326)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4fa [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 55927, Dst Port: 53
Source Port: 55927
Destination Port: 53
Length: 38
Checksum: 0x54e4 [unverified]
[Checksum Status: Unverified]
[Stream index: 68]
Domain Name System (query)
Transaction ID: 0x979f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... 0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0... = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
alum.mit.edu: type A, class IN
Name: alum.mit.edu
[Name Length: 12]

[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 1553]

No.	Time	Source	Destination	Protocol	Length	Info
1544	2018-10-17 16:36:36.257486	202.117.112.3	10.173.88.157	DNS	320	Standard query response

0xba7f A meche.mit.edu A 18.9.44.34 NS m.edu-servers.net NS g.edu-servers.net NS h.edu-servers.net NS j.edu-servers.net NS a.edu-servers.net NS l.edu-servers.net NS i.edu-servers.net NS c.edu-servers.net NS d.edu-servers.net NS f.edu-servers.net NS e.edu-servers.net NS b.edu-servers.net NS k.edu-servers.net

Frame 1544: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.257486000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.257486000 seconds
[Time delta from previous captured frame: 0.008128000 seconds]
[Time delta from previous displayed frame: 0.008128000 seconds]
[Time since reference or first frame: 6.014019000 seconds]
Frame Number: 1544
Frame Length: 320 bytes (2560 bits)
Capture Length: 320 bytes (2560 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 300
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
. 0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 298
Identification: 0x521b (21019)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
.0.... = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de5 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 52388
Source Port: 53
Destination Port: 52388
Length: 278
Checksum: 0xed12 [unverified]
[Checksum Status: Unverified]
[Stream index: 62]
Domain Name System (response)
Transaction ID: 0xba7f
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.0.... = Authoritative: Server is not an authority for domain

.... 0 = Truncated: Message is not truncated
.... 1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
.... 0... = Z: reserved (0)
.... 00. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... 000 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 13

Additional RRs: 0

Queries

meche.mit.edu: type A, class IN
Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

meche.mit.edu: type A, class IN, addr 18.9.44.34
Name: meche.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.44.34

Authoritative nameservers

edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 19
Name Server: m.edu-servers.net

edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: g.edu-servers.net

edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: h.edu-servers.net

edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: j.edu-servers.net

edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: a.edu-servers.net

edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: l.edu-servers.net

edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: i.edu-servers.net

edu: type NS, class IN, ns c.edu-servers.net

Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: c.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: d.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: k.edu-servers.net

[Request In: 1532]
[Time: 0.055654000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1545	2018-10-17 16:36:36.259832	10.173.88.157	202.117.112.3	DNS	81	Standard query 0xc1c8

A meche.mit.edu

Frame 1545: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.259832000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.259832000 seconds
[Time delta from previous captured frame: 0.002346000 seconds]
[Time delta from previous displayed frame: 0.002346000 seconds]
[Time since reference or first frame: 6.016365000 seconds]
Frame Number: 1545
Frame Length: 81 bytes (648 bits)
Capture Length: 81 bytes (648 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x000)
Session ID: 0x629d
Payload Length: 61
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.0000 ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 59
Identification: 0x37f7 (14327)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4f8 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 56657, Dst Port: 53
Source Port: 56657
Destination Port: 53
Length: 39
Checksum: 0x179b [unverified]
[Checksum Status: Unverified]
[Stream index: 69]
Domain Name System (query)
Transaction ID: 0xc1c8
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0.. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
meche.mit.edu: type A, class IN
Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1546]
No. Time Source Destination Protocol Length Info
1546 2018-10-17 16:36:36.260902 202.117.112.3 10.173.88.157 DNS 320 Standard query response
0xc1c8 A meche.mit.edu A 18.9.44.34 NS i.edu-servers.net NS m.edu-servers.net NS h.edu-servers.net NS j.edu-servers.net NS l.edu-servers.net NS a.edu-servers.net NS f.edu-servers.net NS k.edu-servers.net NS b.edu-servers.net NS e.edu-servers.net NS c.edu-servers.net NS d.edu-servers.net NS g.edu-servers.net
Frame 1546: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.260902000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.260902000 seconds
[Time delta from previous captured frame: 0.001070000 seconds]
[Time delta from previous displayed frame: 0.001070000 seconds]
[Time since reference or first frame: 6.017435000 seconds]
Frame Number: 1546
Frame Length: 320 bytes (2560 bits)
Capture Length: 320 bytes (2560 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 300

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 298
Identification: 0x521c (21020)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de4 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 56657
Source Port: 53
Destination Port: 56657
Length: 278
Checksum: 0xd918 [unverified]
[Checksum Status: Unverified]
[Stream index: 69]
Domain Name System (response)
Transaction ID: 0xc1c8
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0... = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
meche.mit.edu: type A, class IN
Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
meche.mit.edu: type A, class IN, addr 18.9.44.34
Name: meche.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1800
Data length: 4
Address: 18.9.44.34
Authoritative nameservers
edu: type NS, class IN, ns i.edu-servers.net
Name: edu

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 19
Name Server: i.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: m.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: h.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: a.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: k.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: c.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
Name: edu

Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: d.edu-servers.net
edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: g.edu-servers.net
[Request In: 1545]
[Time: 0.001070000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1547	2018-10-17 16:36:36.262756	10.173.88.157	202.117.112.3	DNS	81	Standard query 0x3f1d

AAAA meche.mit.edu
Frame 1547: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.262756000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.262756000 seconds
[Time delta from previous captured frame: 0.001854000 seconds]
[Time delta from previous displayed frame: 0.001854000 seconds]
[Time since reference or first frame: 6.019289000 seconds]
Frame Number: 1547
Frame Length: 81 bytes (648 bits)
Capture Length: 81 bytes (648 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 61
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 59
Identification: 0x37f8 (14328)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4f7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 50964, Dst Port: 53
Source Port: 50964
Destination Port: 53
Length: 39
Checksum: 0x9583 [unverified]

[Checksum Status: Unverified]
[Stream index: 70]
Domain Name System (query)
Transaction ID: 0x3f1d
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 meche.mit.edu: type AAAA, class IN
 Name: meche.mit.edu
 [Name Length: 13]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1557]
No. Time Source Destination Protocol Length Info
1548 2018-10-17 16:36:36.264023 218.30.19.40 10.173.88.157 DNS 149 Standard query response
0xcd9 AAAA malgosia.mit.edu SOA use2.akam.net
Frame 1548: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.264023000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.264023000 seconds
[Time delta from previous captured frame: 0.001267000 seconds]
[Time delta from previous displayed frame: 0.001267000 seconds]
[Time since reference or first frame: 6.020556000 seconds]
Frame Number: 1548
Frame Length: 149 bytes (1192 bits)
Capture Length: 149 bytes (1192 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 129
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 127
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)

Header checksum: 0xf0dd [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 59337
Source Port: 53
Destination Port: 59337
Length: 107
Checksum: 0x24ea [unverified]
[Checksum Status: Unverified]
[Stream index: 63]
Domain Name System (response)
Transaction ID: 0xcdb9
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... ..0.... = Truncated: Message is not truncated
.... ...1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
 malgosia.mit.edu: type AAAA, class IN
 Name: malgosia.mit.edu
 [Name Length: 16]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
Authoritative nameservers
 mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)
 [Request In: 1533]
 [Time: 0.058942000 seconds]
No. Time Source Destination Protocol Length Info
1549 2018-10-17 16:36:36.268597 218.30.19.40 10.173.88.157 DNS 141 Standard query response
0x8e27 AAAA mitadmissions.org AAAA 2606:4700:20::6818:156d AAAA 2606:4700:20::6818:166d
Frame 1549: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.268597000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.268597000 seconds
[Time delta from previous captured frame: 0.004574000 seconds]
[Time delta from previous displayed frame: 0.004574000 seconds]
[Time since reference or first frame: 6.025130000 seconds]
Frame Number: 1549
Frame Length: 141 bytes (1128 bits)
Capture Length: 141 bytes (1128 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0.... = LG bit: Globally unique address (factory default)
.... ...0.... = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 121

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 119
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0.... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0e5 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 59315
Source Port: 53
Destination Port: 59315
Length: 99
Checksum: 0x6fce [unverified]
[Checksum Status: Unverified]
[Stream index: 57]

Domain Name System (response)
Transaction ID: 0x8e27
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
mitadmissions.org: type AAAA, class IN
Name: mitadmissions.org
[Name Length: 17]
[Label Count: 2]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Answers
mitadmissions.org: type AAAA, class IN, addr 2606:4700:20::6818:156d
Name: mitadmissions.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2606:4700:20::6818:156d

mitadmissions.org: type AAAA, class IN, addr 2606:4700:20::6818:166d
Name: mitadmissions.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16

AAAA Address: 2606:4700:20::6818:166d
[Request In: 1515]
[Time: 0.727192000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1550	2018-10-17 16:36:36.280171	218.30.19.40	10.173.88.157	DNS	97	Standard query response

0xba7f A meche.mit.edu A 18.9.44.34
Frame 1550: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.280171000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.280171000 seconds
[Time delta from previous captured frame: 0.011574000 seconds]
[Time delta from previous displayed frame: 0.011574000 seconds]
[Time since reference or first frame: 6.036704000 seconds]
Frame Number: 1550
Frame Length: 97 bytes (776 bits)
Capture Length: 97 bytes (776 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 77
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 75
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf111 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 52388
Source Port: 53
Destination Port: 52388
Length: 55
Checksum: 0xb61c [unverified]
[Checksum Status: Unverified]
[Stream index: 64]
Domain Name System (response)
Transaction ID: 0xba7f
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries

....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

meche.mit.edu: type A, class IN
 Name: meche.mit.edu
 [Name Length: 13]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

Answers

meche.mit.edu: type A, class IN, addr 18.9.44.34

 Name: meche.mit.edu

 Type: A (Host Address) (1)

 Class: IN (0x0001)

 Time to live: 1800

 Data length: 4

 Address: 18.9.44.34

[Request In: 1535]

[Time: 0.055231000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1551	2018-10-17 16:36:36.285336	10.173.88.157	218.30.19.40	DNS	80	Standard query 0x979f

A alum.mit.edu

Frame 1551: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.285336000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.285336000 seconds

[Time delta from previous captured frame: 0.005165000 seconds]

[Time delta from previous displayed frame: 0.005165000 seconds]

[Time since reference or first frame: 6.041869000 seconds]

Frame Number: 1551

Frame Length: 80 bytes (640 bits)

Capture Length: 80 bytes (640 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 60

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 58

Identification: 0x6284 (25220)

Flags: 0x0000

0... = Reserved bit: Not set

.0... = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79e [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 55927, Dst Port: 53
Source Port: 55927
Destination Port: 53
Length: 38
Checksum: 0xa216 [unverified]
[Checksum Status: Unverified]
[Stream index: 71]
Domain Name System (query)
Transaction ID: 0x979f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 alum.mit.edu: type A, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1560]
No. Time Source Destination Protocol Length Info
1552 2018-10-17 16:36:36.285438 10.173.88.157 218.30.19.40 DNS 81 Standard query 0x3f1d
AAAA meche.mit.edu
Frame 1552: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.285438000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.285438000 seconds
[Time delta from previous captured frame: 0.000102000 seconds]
[Time delta from previous displayed frame: 0.000102000 seconds]
[Time since reference or first frame: 6.041971000 seconds]
Frame Number: 1552
Frame Length: 81 bytes (648 bits)
Capture Length: 81 bytes (648 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 61
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 59
Identification: 0x6285 (25221)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79c [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 50964, Dst Port: 53
Source Port: 50964
Destination Port: 53
Length: 39
Checksum: 0xe2b5 [unverified]
[Checksum Status: Unverified]
[Stream index: 72]
Domain Name System (query)
Transaction ID: 0x3f1d
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively
.0.. = Z: reserved (0)
.0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
meche.mit.edu: type AAAA, class IN
 Name: meche.mit.edu
 [Name Length: 13]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1562]

No.	Time	Source	Destination	Protocol	Length	Info
1553	2018-10-17 16:36:36.297314	202.117.112.3	10.173.88.157	DNS	319	Standard query response

0x979f A alum.mit.edu A 23.11.16.40 NS k.edu-servers.net NS j.edu-servers.net NS e.edu-servers.net NS l.edu-servers.net NS d.edu-servers.net NS c.edu-servers.net NS m.edu-servers.net NS f.edu-servers.net NS h.edu-servers.net NS a.edu-servers.net NS i.edu-servers.net NS b.edu-servers.net NS g.edu-servers.net

Frame 1553: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.297314000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.297314000 seconds
[Time delta from previous captured frame: 0.011876000 seconds]
[Time delta from previous displayed frame: 0.011876000 seconds]
[Time since reference or first frame: 6.053847000 seconds]
Frame Number: 1553
Frame Length: 319 bytes (2552 bits)
Capture Length: 319 bytes (2552 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.0. = LG bit: Globally unique address (factory default)
.0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.0. = LG bit: Globally unique address (factory default)
.0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session

0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 299
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 297
Identification: 0x521d (21021)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de4 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55927
Source Port: 53
Destination Port: 55927
Length: 277
Checksum: 0xf38e [unverified]
[Checksum Status: Unverified]
[Stream index: 68]
Domain Name System (response)
Transaction ID: 0x979f
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
alum.mit.edu: type A, class IN
Name: alum.mit.edu
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
alum.mit.edu: type A, class IN, addr 23.11.16.40
Name: alum.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 23.11.16.40
Authoritative nameservers
edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 19
Name Server: k.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 172717
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns e.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: e.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: d.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: c.edu-servers.net
edu: type NS, class IN, ns m.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: m.edu-servers.net
edu: type NS, class IN, ns f.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: f.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: h.edu-servers.net
edu: type NS, class IN, ns a.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: a.edu-servers.net
edu: type NS, class IN, ns i.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: i.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns g.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)

Time to live: 172717
Data length: 4
Name Server: g.edu-servers.net
[Request In: 1543]
[Time: 0.047956000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1554	2018-10-17 16:36:36.301011	10.173.88.157	202.117.112.3	DNS	80	Standard query 0x9f8f

A alum.mit.edu

Frame 1554: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.301011000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.301011000 seconds
[Time delta from previous captured frame: 0.003697000 seconds]
[Time delta from previous displayed frame: 0.003697000 seconds]
[Time since reference or first frame: 6.057544000 seconds]
Frame Number: 1554
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
. 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 60

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
. 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 58
Identification: 0x37f9 (14329)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4f7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 62857, Dst Port: 53
Source Port: 62857
Destination Port: 53
Length: 38
Checksum: 0x31e2 [unverified]
[Checksum Status: Unverified]
[Stream index: 73]
Domain Name System (query)
Transaction ID: 0x9f8f
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.0. = Truncated: Message is not truncated
.1 = Recursion desired: Do query recursively

....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 alum.mit.edu: type A, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1555]
No. Time Source Destination Protocol Length Info
1555 2018-10-17 16:36:36.301914 202.117.112.3 10.173.88.157 DNS 319 Standard query response
0x9f8f A alum.mit.edu A 23.11.16.40 NS f.edu-servers.net NS g.edu-servers.net NS m.edu-servers.net NS a.edu-servers.net NS e.edu-servers.net NS i.edu-servers.net NS l.edu-servers.net NS k.edu-servers.net NS j.edu-servers.net NS c.edu-servers.net NS d.edu-servers.net NS b.edu-servers.net NS h.edu-servers.net
Frame 1555: 319 bytes on wire (2552 bits), 319 bytes captured (2552 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.301914000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.301914000 seconds
[Time delta from previous captured frame: 0.000903000 seconds]
[Time delta from previous displayed frame: 0.000903000 seconds]
[Time since reference or first frame: 6.058447000 seconds]
Frame Number: 1555
Frame Length: 319 bytes (2552 bits)
Capture Length: 319 bytes (2552 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 299
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 297
Identification: 0x521e (21022)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8de3 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 62857
Source Port: 53
Destination Port: 62857

Length: 277
Checksum: 0xcb91 [unverified]
[Checksum Status: Unverified]
[Stream index: 73]
Domain Name System (response)
Transaction ID: 0x9f8f
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
 alum.mit.edu: type A, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
Answers
 alum.mit.edu: type A, class IN, addr 23.11.16.40
 Name: alum.mit.edu
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 300
 Data length: 4
 Address: 23.11.16.40
Authoritative nameservers
 edu: type NS, class IN, ns f.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717
 Data length: 19
 Name Server: f.edu-servers.net
 edu: type NS, class IN, ns g.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717
 Data length: 4
 Name Server: g.edu-servers.net
 edu: type NS, class IN, ns m.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717
 Data length: 4
 Name Server: m.edu-servers.net
 edu: type NS, class IN, ns a.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717
 Data length: 4
 Name Server: a.edu-servers.net
 edu: type NS, class IN, ns e.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717
 Data length: 4
 Name Server: e.edu-servers.net
 edu: type NS, class IN, ns i.edu-servers.net
 Name: edu
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 172717

```
Data length: 4
Name Server: i.edu-servers.net
edu: type NS, class IN, ns l.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: l.edu-servers.net
edu: type NS, class IN, ns k.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: k.edu-servers.net
edu: type NS, class IN, ns j.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: j.edu-servers.net
edu: type NS, class IN, ns c.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: c.edu-servers.net
edu: type NS, class IN, ns d.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: d.edu-servers.net
edu: type NS, class IN, ns b.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: b.edu-servers.net
edu: type NS, class IN, ns h.edu-servers.net
Name: edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 172717
Data length: 4
Name Server: h.edu-servers.net
[Request In: 1554]
[Time: 0.000903000 seconds]
No. Time Source Destination Protocol Length Info
1556 2018-10-17 16:36:36.304356 10.173.88.157 202.117.112.3 DNS 80 Standard query 0x87ae
AAAA alum.mit.edu
Frame 1556: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.304356000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.304356000 seconds
[Time delta from previous captured frame: 0.002442000 seconds]
[Time delta from previous displayed frame: 0.002442000 seconds]
[Time since reference or first frame: 6.060889000 seconds]
Frame Number: 1556
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
```

.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 60

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 58
Identification: 0x37fa (14330)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4f6 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 54427, Dst Port: 53
Source Port: 54427
Destination Port: 53
Length: 38
Checksum: 0x6a96 [unverified]
[Checksum Status: Unverified]
[Stream index: 74]

Domain Name System (query)
Transaction ID: 0x87ae
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0.. = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 alum.mit.edu: type AAAA, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1563]

No.	Time	Source	Destination	Protocol	Length	Info
1557	2018-10-17 16:36:36.318589	202.117.112.3	10.173.88.157	DNS	146	Standard query response

Frame 1557: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.318589000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.318589000 seconds
[Time delta from previous captured frame: 0.014233000 seconds]
[Time delta from previous displayed frame: 0.014233000 seconds]
[Time since reference or first frame: 6.075122000 seconds]
Frame Number: 1557
Frame Length: 146 bytes (1168 bits)

Capture Length: 146 bytes (1168 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 126

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 124
Identification: 0x521f (21023)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e8f [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 50964
Source Port: 53
Destination Port: 50964
Length: 104
Checksum: 0x5992 [unverified]
[Checksum Status: Unverified]
[Stream index: 70]

Domain Name System (response)
Transaction ID: 0x3f1d
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
meche.mit.edu: type AAAA, class IN
Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
Name: mit.edu

Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 1800
Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)
[Request In: 1547]
[Time: 0.055833000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1558	2018-10-17 16:36:36.321590	10.173.88.157	202.117.112.3	DNS	92	Standard query 0xf47a

A www.povertyactionlab.org
Frame 1558: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.321590000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.321590000 seconds
[Time delta from previous captured frame: 0.003001000 seconds]
[Time delta from previous displayed frame: 0.003001000 seconds]
[Time since reference or first frame: 6.078123000 seconds]
Frame Number: 1558
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 70
Identification: 0x37fb (14331)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
..0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e9 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 53648, Dst Port: 53
Source Port: 53648
Destination Port: 53
Length: 50
Checksum: 0xdbaf [unverified]
[Checksum Status: Unverified]

[Stream index: 75]
Domain Name System (query)
Transaction ID: 0xf47a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... ..0. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.povertyactionlab.org: type A, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1583]
No. Time Source Destination Protocol Length Info
1559 2018-10-17 16:36:36.330532 10.173.88.157 218.30.19.40 DNS 80 Standard query 0x87ae
AAAA alum.mit.edu
Frame 1559: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.330532000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.330532000 seconds
[Time delta from previous captured frame: 0.008942000 seconds]
[Time delta from previous displayed frame: 0.008942000 seconds]
[Time since reference or first frame: 6.087065000 seconds]
Frame Number: 1559
Frame Length: 80 bytes (640 bits)
Capture Length: 80 bytes (640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 60
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 58
Identification: 0x6286 (25222)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
..0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc79c [validation disabled]

[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 54427, Dst Port: 53
Source Port: 54427
Destination Port: 53
Length: 38
Checksum: 0xb7c8 [unverified]
[Checksum Status: Unverified]
[Stream index: 76]
Domain Name System (query)
Transaction ID: 0x87ae
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1. = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 alum.mit.edu: type AAAA, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 [Response In: 1566]
No. Time Source Destination Protocol Length Info
1560 2018-10-17 16:36:36.338310 218.30.19.40 10.173.88.157 DNS 96 Standard query response
0x979f A alum.mit.edu A 23.11.16.40
Frame 1560: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.338310000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.338310000 seconds
[Time delta from previous captured frame: 0.007778000 seconds]
[Time delta from previous displayed frame: 0.007778000 seconds]
[Time since reference or first frame: 6.094843000 seconds]
Frame Number: 1560
Frame Length: 96 bytes (768 bits)
Capture Length: 96 bytes (768 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 76
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 74

Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf112 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 55927
Source Port: 53
Destination Port: 55927
Length: 54
Checksum: 0x3903 [unverified]
[Checksum Status: Unverified]
[Stream index: 71]
Domain Name System (response)
Transaction ID: 0x979f
Flags: 0x8180 Standard query response, No error
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
. 0. = Authoritative: Server is not an authority for domain
. 0. = Truncated: Message is not truncated
. 1.... = Recursion desired: Do query recursively
. 1.... = Recursion available: Server can do recursive queries
. 0... = Z: reserved (0)
. 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
. 0.... = Non-authenticated data: Unacceptable
. 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
alum.mit.edu: type A, class IN
Name: alum.mit.edu
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
alum.mit.edu: type A, class IN, addr 23.11.16.40
Name: alum.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 23.11.16.40
[Request In: 1551]
[Time: 0.052974000 seconds]
No. Time Source Destination Protocol Length Info
1561 2018-10-17 16:36:36.344356 10.173.88.157 218.30.19.40 DNS 92 Standard query 0xf47a
A www.povertyactionlab.org
Frame 1561: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.344356000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.344356000 seconds
[Time delta from previous captured frame: 0.006046000 seconds]
[Time delta from previous displayed frame: 0.006046000 seconds]
[Time since reference or first frame: 6.100889000 seconds]
Frame Number: 1561
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ..0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 70
Identification: 0x6287 (25223)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc78f [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40
User Datagram Protocol, Src Port: 53648, Dst Port: 53
Source Port: 53648
Destination Port: 53
Length: 50
Checksum: 0x28e2 [unverified]
[Checksum Status: Unverified]
[Stream index: 77]
Domain Name System (query)
Transaction ID: 0xf47a
Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0.. = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 www.povertyactionlab.org: type A, class IN
 Name: www.povertyactionlab.org
 [Name Length: 24]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1588]
No. Time Source Destination Protocol Length Info
1562 2018-10-17 16:36:36.344887 218.30.19.40 10.173.88.157 DNS 146 Standard query response
0x3f1d AAAA meche.mit.edu SOA use2.akam.net
Frame 1562: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.344887000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.344887000 seconds
[Time delta from previous captured frame: 0.000531000 seconds]
[Time delta from previous displayed frame: 0.000531000 seconds]
[Time since reference or first frame: 6.101420000 seconds]
Frame Number: 1562
Frame Length: 146 bytes (1168 bits)

Capture Length: 146 bytes (1168 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 126

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 124
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0e0 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 50964
Source Port: 53
Destination Port: 50964
Length: 104
Checksum: 0xa6c4 [unverified]
[Checksum Status: Unverified]
[Stream index: 72]

Domain Name System (response)
Transaction ID: 0x3f1d
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
meche.mit.edu: type AAAA, class IN
Name: meche.mit.edu
[Name Length: 13]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
Name: mit.edu

Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 1800
Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)
[Request In: 1552]
[Time: 0.059449000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1563	2018-10-17 16:36:36.352704	202.117.112.3	10.173.88.157	DNS	145	Standard query response

0x87ae AAAA alum.mit.edu SOA use2.akam.net

Frame 1563: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.352704000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.352704000 seconds
[Time delta from previous captured frame: 0.007817000 seconds]
[Time delta from previous displayed frame: 0.007817000 seconds]
[Time since reference or first frame: 6.109237000 seconds]
Frame Number: 1563
Frame Length: 145 bytes (1160 bits)
Capture Length: 145 bytes (1160 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 125

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 123
Identification: 0x5220 (21024)
Flags: 0x0000
0.... = Reserved bit: Not set
.0.... = Don't fragment: Not set
..0.... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e8f [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 54427
Source Port: 53
Destination Port: 54427
Length: 103
Checksum: 0xfcfd8 [unverified]
[Checksum Status: Unverified]

[Stream index: 74]
Domain Name System (response)
Transaction ID: 0x87ae
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0.... = Authoritative: Server is not an authority for domain
.... .0.... = Truncated: Message is not truncated
.... .1.... = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.... = Z: reserved (0)
....0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0.... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
 alum.mit.edu: type AAAA, class IN
 Name: alum.mit.edu
 [Name Length: 12]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
Authoritative nameservers
 mit.edu: type SOA, class IN, mname use2.akam.net
 Name: mit.edu
 Type: SOA (Start Of a zone of Authority) (6)
 Class: IN (0x0001)
 Time to live: 1800
 Data length: 53
 Primary name server: use2.akam.net
 Responsible authority's mailbox: network-request.mit.edu
 Serial Number: 11252
 Refresh Interval: 900 (15 minutes)
 Retry Interval: 900 (15 minutes)
 Expire limit: 3600000 (41 days, 16 hours)
 Minimum TTL: 3600 (1 hour)
 [Request In: 1556]
 [Time: 0.048348000 seconds]
No. Time Source Destination Protocol Length Info
1564 2018-10-17 16:36:36.354016 10.173.88.157 202.117.112.3 DNS 88 Standard query 0x6a7e
A mitpkg.wordpress.com
Frame 1564: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:36.354016000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765396.354016000 seconds
 [Time delta from previous captured frame: 0.001312000 seconds]
 [Time delta from previous displayed frame: 0.001312000 seconds]
 [Time since reference or first frame: 6.110549000 seconds]
 Frame Number: 1564
 Frame Length: 88 bytes (704 bits)
 Capture Length: 88 bytes (704 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0.... = LG bit: Globally unique address (factory default)
 0.... = IG bit: Individual address (unicast)
 Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0.... = LG bit: Globally unique address (factory default)
 0.... = IG bit: Individual address (unicast)
 Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d

Payload Length: 68
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 66
Identification: 0x37fc (14332)
Flags: 0x0000
0.... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0.. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4ec [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 51573, Dst Port: 53
Source Port: 51573
Destination Port: 53
Length: 46
Checksum: 0xe21f [unverified]
[Checksum Status: Unverified]
[Stream index: 78]
Domain Name System (query)
Transaction ID: 0x6a7e
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1.... = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mitpkg.wordpress.com: type A, class IN
Name: mitpkg.wordpress.com
[Name Length: 20]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1567]
No. Time Source Destination Protocol Length Info
1565 2018-10-17 16:36:36.379706 10.173.88.157 218.30.19.40 DNS 88 Standard query 0x6a7e
A mitpkg.wordpress.com
Frame 1565: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.379706000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.379706000 seconds
[Time delta from previous captured frame: 0.025690000 seconds]
[Time delta from previous displayed frame: 0.025690000 seconds]
[Time since reference or first frame: 6.136239000 seconds]
Frame Number: 1565
Frame Length: 88 bytes (704 bits)
Capture Length: 88 bytes (704 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 68

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 66

Identification: 0x6288 (25224)

Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0xc792 [validation disabled]
[Header checksum status: Unverified]

Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 51573, Dst Port: 53
Source Port: 51573
Destination Port: 53
Length: 46

Checksum: 0x2f52 [unverified]
[Checksum Status: Unverified]
[Stream index: 79]

Domain Name System (query)
Transaction ID: 0x6a7e
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mitpkg.wordpress.com: type A, class IN
Name: mitpkg.wordpress.com
[Name Length: 20]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1572]

No.	Time	Source	Destination	Protocol	Length	Info
1566	2018-10-17 16:36:36.390815	218.30.19.40	10.173.88.157	DNS	145	Standard query response

Frame 1566: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.390815000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.390815000 seconds
[Time delta from previous captured frame: 0.011109000 seconds]
[Time delta from previous displayed frame: 0.011109000 seconds]
[Time since reference or first frame: 6.147348000 seconds]
Frame Number: 1566
Frame Length: 145 bytes (1160 bits)
Capture Length: 145 bytes (1160 bits)
[Frame is marked: False]
[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 125

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 123
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0.... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0e1 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 54427
Source Port: 53
Destination Port: 54427
Length: 103
Checksum: 0x4a0b [unverified]
[Checksum Status: Unverified]
[Stream index: 76]

Domain Name System (response)
Transaction ID: 0x87ae
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... 1.... = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
alum.mit.edu: type AAAA, class IN
Name: alum.mit.edu
[Name Length: 12]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Authoritative nameservers
mit.edu: type SOA, class IN, mname use2.akam.net
Name: mit.edu
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 1800

Data length: 53
Primary name server: use2.akam.net
Responsible authority's mailbox: network-request.mit.edu
Serial Number: 11252
Refresh Interval: 900 (15 minutes)
Retry Interval: 900 (15 minutes)
Expire limit: 3600000 (41 days, 16 hours)
Minimum TTL: 3600 (1 hour)

[Request In: 1559]
[Time: 0.060283000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1567	2018-10-17 16:36:36.516393	202.117.112.3	10.173.88.157	DNS	361	Standard query response

0x6a7e A mitpkg.wordpress.com CNAME lb.wordpress.com A 192.0.78.13 A 192.0.78.12 NS a.gtld-servers.net NS g.gtld-servers.net NS h.gtld-servers.net NS j.gtld-servers.net NS e.gtld-servers.net NS f.gtld-servers.net NS i.gtld-servers.net NS l.gtld-servers.net NS b.gtld-servers.net NS d.gtld-servers.net NS m.gtld-servers.net NS k.gtld-servers.net NS c.gtld-servers.net

Frame 1567: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.516393000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.516393000 seconds
[Time delta from previous captured frame: 0.125578000 seconds]
[Time delta from previous displayed frame: 0.125578000 seconds]
[Time since reference or first frame: 6.272926000 seconds]
Frame Number: 1567
Frame Length: 361 bytes (2888 bits)
Capture Length: 361 bytes (2888 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 341

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 339
Identification: 0x5221 (21025)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8db6 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 51573
Source Port: 53
Destination Port: 51573
Length: 319
Checksum: 0x975c [unverified]
[Checksum Status: Unverified]
[Stream index: 78]

Domain Name System (response)
Transaction ID: 0x6a7e
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 13
Additional RRs: 0
Queries
mitpkg.wordpress.com: type A, class IN
Name: mitpkg.wordpress.com
[Name Length: 20]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
mitpkg.wordpress.com: type CNAME, class IN, cname lb.wordpress.com
Name: mitpkg.wordpress.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 14400
Data length: 5
CNAME: lb.wordpress.com
lb.wordpress.com: type A, class IN, addr 192.0.78.13
Name: lb.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.13
lb.wordpress.com: type A, class IN, addr 192.0.78.12
Name: lb.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.12
Authoritative nameservers
com: type NS, class IN, ns a.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 20
Name Server: a.gtld-servers.net
com: type NS, class IN, ns g.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: g.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: h.gtld-servers.net
com: type NS, class IN, ns j.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: j.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
Name: com

Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: e.gtld-servers.net
 com: type NS, class IN, ns f.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: f.gtld-servers.net
 com: type NS, class IN, ns i.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: i.gtld-servers.net
 com: type NS, class IN, ns l.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: l.gtld-servers.net
 com: type NS, class IN, ns b.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: b.gtld-servers.net
 com: type NS, class IN, ns d.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: d.gtld-servers.net
 com: type NS, class IN, ns m.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: m.gtld-servers.net
 com: type NS, class IN, ns k.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: k.gtld-servers.net
 com: type NS, class IN, ns c.gtld-servers.net
 Name: com
 Type: NS (authoritative Name Server) (2)
 Class: IN (0x0001)
 Time to live: 169179
 Data length: 4
 Name Server: c.gtld-servers.net

[Request In: 1564]

[Time: 0.162377000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1568	2018-10-17 16:36:36.518574	10.173.88.157	202.117.112.3	DNS	84	Standard query 0x9729

A lb.wordpress.com

Frame 1568: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.518574000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.518574000 seconds

[Time delta from previous captured frame: 0.002181000 seconds]

[Time delta from previous displayed frame: 0.002181000 seconds]

[Time since reference or first frame: 6.275107000 seconds]

Frame Number: 1568

Frame Length: 84 bytes (672 bits)
 Capture Length: 84 bytes (672 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:etherype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
0 = LG bit: Globally unique address (factory default)
0 = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
0 = LG bit: Globally unique address (factory default)
0 = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
 Code: Session Data (0x00)
 Session ID: 0x629d
 Payload Length: 64

Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
 Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 62
 Identification: 0x37fd (14333)
 Flags: 0x0000
 0... = Reserved bit: Not set
 .0... = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0xa4ef [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.173.88.157
 Destination: 202.117.112.3

User Datagram Protocol, Src Port: 63248, Dst Port: 53
 Source Port: 63248
 Destination Port: 53
 Length: 42
 Checksum: 0x6ac2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 80]

Domain Name System (query)
 Transaction ID: 0x9729
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
0. = Truncated: Message is not truncated
1 = Recursion desired: Do query recursively
0.. = Z: reserved (0)
0 = Non-authenticated data: Unacceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 lb.wordpress.com: type A, class IN
 Name: lb.wordpress.com
 [Name Length: 16]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1569]

No.	Time	Source	Destination	Protocol	Length	Info										
1569	2018-10-17 16:36:36.519609	202.117.112.3	10.173.88.157	DNS	340	Standard query response										
0x9729	A	lb.wordpress.com	A 192.0.78.12	NS d.gtld-servers.net	NS 1.gtld-servers.net	NS f.gtld-servers.net	NS m.gtld-servers.net	NS g.gtld-servers.net	NS b.gtld-servers.net	NS k.gtld-servers.net	NS j.gtld-servers.net	NS c.gtld-servers.net	NS e.gtld-servers.net	NS i.gtld-servers.net	NS h.gtld-servers.net	NS a.gtld-servers.net

Frame 1569: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.519609000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.519609000 seconds
[Time delta from previous captured frame: 0.001035000 seconds]
[Time delta from previous displayed frame: 0.001035000 seconds]
[Time since reference or first frame: 6.276142000 seconds]
Frame Number: 1569
Frame Length: 340 bytes (2720 bits)
Capture Length: 340 bytes (2720 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 320
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 318
Identification: 0x5222 (21026)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dca [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 63248
Source Port: 53
Destination Port: 63248
Length: 298
Checksum: 0x5d57 [unverified]
[Checksum Status: Unverified]
[Stream index: 80]
Domain Name System (response)
Transaction ID: 0x9729
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0... = Z: reserved (0)
 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
 0.... = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2

Authority RRs: 13

Additional RRs: 0

Queries

lb.wordpress.com: type A, class IN
Name: lb.wordpress.com
[Name Length: 16]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

lb.wordpress.com: type A, class IN, addr 192.0.78.12

Name: lb.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.12

lb.wordpress.com: type A, class IN, addr 192.0.78.13

Name: lb.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.13

Authoritative nameservers

com: type NS, class IN, ns d.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 20
Name Server: d.gtld-servers.net

com: type NS, class IN, ns l.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: l.gtld-servers.net

com: type NS, class IN, ns f.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: f.gtld-servers.net

com: type NS, class IN, ns m.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: m.gtld-servers.net

com: type NS, class IN, ns g.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: g.gtld-servers.net

com: type NS, class IN, ns b.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: b.gtld-servers.net

com: type NS, class IN, ns k.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: k.gtld-servers.net

com: type NS, class IN, ns j.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: j.gtld-servers.net
com: type NS, class IN, ns c.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: c.gtld-servers.net
com: type NS, class IN, ns e.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: e.gtld-servers.net
com: type NS, class IN, ns i.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: i.gtld-servers.net
com: type NS, class IN, ns h.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: h.gtld-servers.net
com: type NS, class IN, ns a.gtld-servers.net
Name: com
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169179
Data length: 4
Name Server: a.gtld-servers.net

[Request In: 1568]

[Time: 0.001035000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1570	2018-10-17 16:36:36.520287	10.173.88.157	202.117.112.3	DNS	84	Standard query 0x2ad1

AAAA lb.wordpress.com

Frame 1570: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:36.520287000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.520287000 seconds

[Time delta from previous captured frame: 0.000678000 seconds]

[Time delta from previous displayed frame: 0.000678000 seconds]

[Time since reference or first frame: 6.276820000 seconds]

Frame Number: 1570

Frame Length: 84 bytes (672 bits)

Capture Length: 84 bytes (672 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 64
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 62
Identification: 0x37fe (14334)
Flags: 0x0000
0.... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0.. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4ee [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 59879, Dst Port: 53
Source Port: 59879
Destination Port: 53
Length: 42
Checksum: 0xe428 [unverified]
[Checksum Status: Unverified]
[Stream index: 81]
Domain Name System (query)
Transaction ID: 0x2ad1
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1.... = Recursion desired: Do query recursively
.... .0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
lb.wordpress.com: type AAAA, class IN
Name: lb.wordpress.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1578]
No. Time Source Destination Protocol Length Info
1571 2018-10-17 16:36:36.541239 10.173.88.157 218.30.19.40 DNS 84 Standard query 0x2ad1
AAAA lb.wordpress.com
Frame 1571: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.541239000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.541239000 seconds
[Time delta from previous captured frame: 0.020952000 seconds]
[Time delta from previous displayed frame: 0.020952000 seconds]
[Time since reference or first frame: 6.297772000 seconds]
Frame Number: 1571
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1

Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 64

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 62
Identification: 0x6289 (25225)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc795 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 59879, Dst Port: 53
Source Port: 59879
Destination Port: 53
Length: 42
Checksum: 0x315b [unverified]
[Checksum Status: Unverified]
[Stream index: 82]

Domain Name System (query)
Transaction ID: 0x2ad1
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
lb.wordpress.com: type AAAA, class IN
Name: lb.wordpress.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1579]

No.	Time	Source	Destination	Protocol	Length	Info
1572	2018-10-17 16:36:36.554557	218.30.19.40	10.173.88.157	DNS	137	Standard query response

0x6a7e A mitpkg.wordpress.com CNAME lb.wordpress.com A 192.0.78.12 A 192.0.78.13
Frame 1572: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.554557000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.554557000 seconds
[Time delta from previous captured frame: 0.013318000 seconds]
[Time delta from previous displayed frame: 0.013318000 seconds]
[Time since reference or first frame: 6.311090000 seconds]
Frame Number: 1572
Frame Length: 137 bytes (1096 bits)
Capture Length: 137 bytes (1096 bits)
[Frame is marked: False]
[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 117

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 115
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0.... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0e9 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 51573
Source Port: 53
Destination Port: 51573
Length: 95
Checksum: 0xcd49 [unverified]
[Checksum Status: Unverified]
[Stream index: 79]

Domain Name System (response)
Transaction ID: 0x6a7e
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... .0. = Truncated: Message is not truncated
.... 1.... = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
mitpkg.wordpress.com: type A, class IN
Name: mitpkg.wordpress.com
[Name Length: 20]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
mitpkg.wordpress.com: type CNAME, class IN, cname lb.wordpress.com
Name: mitpkg.wordpress.com
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 14400

Data length: 5
CNAME: 1b.wordpress.com
1b.wordpress.com: type A, class IN, addr 192.0.78.12
Name: 1b.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.12
1b.wordpress.com: type A, class IN, addr 192.0.78.13
Name: 1b.wordpress.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 242
Data length: 4
Address: 192.0.78.13
[Request In: 1565]
[Time: 0.174851000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1573	2018-10-17 16:36:36.614343	202.117.112.3	10.173.88.157	DNS	85	Standard query response

0xd571 Server failure AAAA www.instagram.com
Frame 1573: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.614343000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.614343000 seconds
[Time delta from previous captured frame: 0.059786000 seconds]
[Time delta from previous displayed frame: 0.059786000 seconds]
[Time since reference or first frame: 6.370876000 seconds]
Frame Number: 1573
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 65
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 63
Identification: 0x5223 (21027)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8ec8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 64089

Source Port: 53
Destination Port: 64089
Length: 43
Checksum: 0x5074 [unverified]
[Checksum Status: Unverified]
[Stream index: 41]
Domain Name System (response)
Transaction ID: 0xd571
Flags: 0x8182 Standard query response, Server failure
1... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
. 0... = Authoritative: Server is not an authority for domain
. 0. = Truncated: Message is not truncated
. 1 = Recursion desired: Do query recursively
. 1... = Recursion available: Server can do recursive queries
. 0... = Z: reserved (0)
. 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
. 0... = Non-authenticated data: Unacceptable
. 0010 = Reply code: Server failure (2)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.instagram.com: type AAAA, class IN
Name: www.instagram.com
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Request In: 986]
[Time: 2.613541000 seconds]
No. Time Source Destination Protocol Length Info
1574 2018-10-17 16:36:36.618463 10.173.88.157 202.117.112.3 DNS 92 Standard query 0x751a
A e3672.ksd.akamaiedge.net
Frame 1574: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.618463000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.618463000 seconds
[Time delta from previous captured frame: 0.004120000 seconds]
[Time delta from previous displayed frame: 0.004120000 seconds]
[Time since reference or first frame: 6.374996000 seconds]
Frame Number: 1574
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
. 0. = LG bit: Globally unique address (factory default)
. 0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 70
Identification: 0x37ff (14335)
Flags: 0x0000
 0... = Reserved bit: Not set
 .0.. = Don't fragment: Not set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e5 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 54462, Dst Port: 53
Source Port: 54462
Destination Port: 53
Length: 50
Checksum: 0x37bf [unverified]
[Checksum Status: Unverified]
[Stream index: 83]
Domain Name System (query)
 Transaction ID: 0x751a
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0... = Opcode: Standard query (0)
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 0... = Z: reserved (0)
 0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
 e3672.ksd.akamaiedge.net: type A, class IN
 Name: e3672.ksd.akamaiedge.net
 [Name Length: 24]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 1575]
No. Time Source Destination Protocol Length Info
1575 2018-10-17 16:36:36.619351 202.117.112.3 10.173.88.157 DNS 329 Standard query response
0x751a A e3672.ksd.akamaiedge.net A 23.11.246.32 NS a.gtld-servers.net NS g.gtld-servers.net NS d.gtld-servers.net NS l.gtld-servers.net NS f.gtld-servers.net NS k.gtld-servers.net NS h.gtld-servers.net NS j.gtld-servers.net NS e.gtld-servers.net NS b.gtld-servers.net NS m.gtld-servers.net NS i.gtld-servers.net NS c.gtld-servers.net
Frame 1575: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits) on interface 0
 Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
 Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
 Encapsulation type: Ethernet (1)
 Arrival Time: Oct 17, 2018 16:36:36.619351000 中国标准时间
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1539765396.619351000 seconds
 [Time delta from previous captured frame: 0.000888000 seconds]
 [Time delta from previous displayed frame: 0.000888000 seconds]
 [Time since reference or first frame: 6.375884000 seconds]
 Frame Number: 1575
 Frame Length: 329 bytes (2632 bits)
 Capture Length: 329 bytes (2632 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0. = LG bit: Globally unique address (factory default)
 0... = IG bit: Individual address (unicast)
 Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0. = LG bit: Globally unique address (factory default)
 0... = IG bit: Individual address (unicast)
 Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1

Code: Session Data (0x000)
Session ID: 0x629d
Payload Length: 309

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 307
Identification: 0x5224 (21028)
Flags: 0x0000
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8dd3 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 54462
Source Port: 53
Destination Port: 54462
Length: 287
Checksum: 0xe8bf [unverified]
[Checksum Status: Unverified]
[Stream index: 83]
Domain Name System (response)
Transaction ID: 0x751a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 0
Queries
e3672.ksd.akamaiedge.net: type A, class IN
Name: e3672.ksd.akamaiedge.net
[Name Length: 24]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
e3672.ksd.akamaiedge.net: type A, class IN, addr 23.11.246.32
Name: e3672.ksd.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 188
Data length: 4
Address: 23.11.246.32
Authoritative nameservers
net: type NS, class IN, ns a.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 17
Name Server: a.gtld-servers.net
net: type NS, class IN, ns g.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4

Name Server: g.gtld-servers.net
net: type NS, class IN, ns d.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: d.gtld-servers.net
net: type NS, class IN, ns l.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: l.gtld-servers.net
net: type NS, class IN, ns f.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: f.gtld-servers.net
net: type NS, class IN, ns k.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: k.gtld-servers.net
net: type NS, class IN, ns h.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: h.gtld-servers.net
net: type NS, class IN, ns j.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: j.gtld-servers.net
net: type NS, class IN, ns e.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: e.gtld-servers.net
net: type NS, class IN, ns b.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: b.gtld-servers.net
net: type NS, class IN, ns m.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: m.gtld-servers.net
net: type NS, class IN, ns i.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4
Name Server: i.gtld-servers.net
net: type NS, class IN, ns c.gtld-servers.net
Name: net
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169186
Data length: 4

Name Server: c.gtld-servers.net
[Request In: 1574]
[Time: 0.000888000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1576	2018-10-17 16:36:36.621237	10.173.88.157	202.117.112.3	DNS	92	Standard query 0x0d4b

AAAA e3672.ksd.akamaiedge.net
Frame 1576: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.621237000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.621237000 seconds
[Time delta from previous captured frame: 0.001886000 seconds]
[Time delta from previous displayed frame: 0.001886000 seconds]
[Time since reference or first frame: 6.377770000 seconds]
Frame Number: 1576
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 70
Identification: 0x3800 (14336)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e4 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3
User Datagram Protocol, Src Port: 52346, Dst Port: 53
Source Port: 52346
Destination Port: 53
Length: 50
Checksum: 0xa7b7 [unverified]
[Checksum Status: Unverified]
[Stream index: 84]
Domain Name System (query)
Transaction ID: 0x0d4b
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
....1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
e3672.ksd.akamaiedge.net: type AAAA, class IN
Name: e3672.ksd.akamaiedge.net
[Name Length: 24]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1577]

No.	Time	Source	Destination	Protocol	Length	Info
1577	2018-10-17 16:36:36.623212	202.117.112.3	10.173.88.157	DNS	155	Standard query response

Frame 1577: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.623212000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.623212000 seconds
[Time delta from previous captured frame: 0.001975000 seconds]
[Time delta from previous displayed frame: 0.001975000 seconds]
[Time since reference or first frame: 6.379745000 seconds]
Frame Number: 1577
Frame Length: 155 bytes (1240 bits)
Capture Length: 155 bytes (1240 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 135
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 133
Identification: 0x5225 (21029)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0xe8e8 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 52346
Source Port: 53
Destination Port: 52346
Length: 113
Checksum: 0xe8e8 [unverified]
[Checksum Status: Unverified]
[Stream index: 84]

Domain Name System (response)
Transaction ID: 0x0d4b
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
e3672.ksd.akamaiedge.net: type AAAA, class IN
Name: e3672.ksd.akamaiedge.net
[Name Length: 24]
[Label Count: 4]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Authoritative nameservers
ksd.akamaiedge.net: type SOA, class IN, mname n0ksd.akamaiedge.net
Name: ksd.akamaiedge.net
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 19
Data length: 51
Primary name server: n0ksd.akamaiedge.net
Responsible authority's mailbox: hostmaster.akamai.com
Serial Number: 1539764416
Refresh Interval: 1000 (16 minutes, 40 seconds)
Retry Interval: 1000 (16 minutes, 40 seconds)
Expire limit: 1000 (16 minutes, 40 seconds)
Minimum TTL: 1800 (30 minutes)
[Request In: 1576]
[Time: 0.001975000 seconds]
No. Time Source Destination Protocol Length Info
1578 2018-10-17 16:36:36.700243 202.117.112.3 10.173.88.157 DNS 137 Standard query response
0x2ad1 AAAA lb.wordpress.com SOA ns1.wordpress.com
Frame 1578: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.700243000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765396.700243000 seconds
[Time delta from previous captured frame: 0.077031000 seconds]
[Time delta from previous displayed frame: 0.077031000 seconds]
[Time since reference or first frame: 6.456776000 seconds]
Frame Number: 1578
Frame Length: 137 bytes (1096 bits)
Capture Length: 137 bytes (1096 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... ..0. = LG bit: Globally unique address (factory default)
.... ...0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 117

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 115
Identification: 0x5226 (21030)
Flags: 0x0000
0.... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e91 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 59879
Source Port: 53
Destination Port: 59879
Length: 95
Checksum: 0x333f [unverified]
[Checksum Status: Unverified]
[Stream index: 81]
Domain Name System (response)
Transaction ID: 0x2ad1
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
lb.wordpress.com: type AAAA, class IN
Name: lb.wordpress.com
[Name Length: 16]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Authoritative nameservers
wordpress.com: type SOA, class IN, mname ns1.wordpress.com
Name: wordpress.com
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 300
Data length: 41
Primary name server: ns1.wordpress.com
Responsible authority's mailbox: mmmmmmm@gmail.com
Serial Number: 2005071858
Refresh Interval: 14400 (4 hours)
Retry Interval: 7200 (2 hours)
Expire limit: 604800 (7 days)
Minimum TTL: 60 (1 minute)
[Request In: 1570]
[Time: 0.179956000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1579	2018-10-17 16:36:36.706601	218.30.19.40	10.173.88.157	DNS	137	Standard query response
0x2ad1	AAAA lb.wordpress.com SOA ns1.wordpress.com					

Frame 1579: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:36.706601000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765396.706601000 seconds
[Time delta from previous captured frame: 0.006358000 seconds]
[Time delta from previous displayed frame: 0.006358000 seconds]
[Time since reference or first frame: 6.463134000 seconds]
Frame Number: 1579
Frame Length: 137 bytes (1096 bits)
Capture Length: 137 bytes (1096 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 117
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 115
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
..0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0e9 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 59879
Source Port: 53
Destination Port: 59879
Length: 95
Checksum: 0x8071 [unverified]
[Checksum Status: Unverified]
[Stream index: 82]
Domain Name System (response)
Transaction ID: 0x2ad1
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0... = Opcode: Standard query (0)
.... .0.. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0. = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
1b.wordpress.com: type AAAA, class IN
Name: 1b.wordpress.com
[Name Length: 16]

[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Authoritative nameservers
wordpress.com: type SOA, class IN, mname ns1.wordpress.com
Name: wordpress.com
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 300
Data length: 41
Primary name server: ns1.wordpress.com
Responsible authority's mailbox: mmmmmmm@gmail.com
Serial Number: 2005071858
Refresh Interval: 14400 (4 hours)
Retry Interval: 7200 (2 hours)
Expire limit: 604800 (7 days)
Minimum TTL: 60 (1 minute)
[Request In: 1571]
[Time: 0.165362000 seconds]
No. Time Source Destination Protocol Length Info
1583 2018-10-17 16:36:37.001987 202.117.112.3 10.173.88.157 DNS 262 Standard query response
0xf47a A www.povertyactionlab.org A 104.25.201.17 A 104.25.200.17 NS a0.org.afilias-nst.info NS b2.org.afilias-nst.org NS
b0.org.afilias-nst.org NS d0.org.afilias-nst.org NS c0.org.afilias-nst.info NS a2.org.afilias-nst.info
Frame 1583: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.001987000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.001987000 seconds
[Time delta from previous captured frame: 0.234292000 seconds]
[Time delta from previous displayed frame: 0.295386000 seconds]
[Time since reference or first frame: 6.758520000 seconds]
Frame Number: 1583
Frame Length: 262 bytes (2096 bits)
Capture Length: 262 bytes (2096 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 242
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 240
Identification: 0x5227 (21031)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e13 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3

Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 53648
Source Port: 53
Destination Port: 53648
Length: 220
Checksum: 0xbecd [unverified]
[Checksum Status: Unverified]
[Stream index: 75]
Domain Name System (response)
Transaction ID: 0xf47a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 0
Queries
www.povertyactionlab.org: type A, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.povertyactionlab.org: type A, class IN, addr 104.25.201.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.201.17
www.povertyactionlab.org: type A, class IN, addr 104.25.200.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.200.17
Authoritative nameservers
org: type NS, class IN, ns a0.org.afiliias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 25
Name Server: a0.org.afiliias-nst.info
org: type NS, class IN, ns b2.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 21
Name Server: b2.org.afiliias-nst.org
org: type NS, class IN, ns b0.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: b0.org.afiliias-nst.org
org: type NS, class IN, ns d0.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: d0.org.afiliias-nst.org
org: type NS, class IN, ns c0.org.afiliias-nst.info

Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: c0.org.afilias-nst.info
org: type NS, class IN, ns a2.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: a2.org.afilias-nst.info

[Request In: 1558]
[Time: 0.680397000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1584	2018-10-17 16:36:37.003367	10.173.88.157	202.117.112.3	DNS	92	Standard query 0x475a

A www.povertyactionlab.org

Frame 1584: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.003367000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.003367000 seconds
[Time delta from previous captured frame: 0.001380000 seconds]
[Time delta from previous displayed frame: 0.001380000 seconds]
[Time since reference or first frame: 6.759900000 seconds]
Frame Number: 1584
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSGP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 70
Identification: 0x3801 (14337)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e3 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 202.117.112.3

User Datagram Protocol, Src Port: 64019, Dst Port: 53
Source Port: 64019
Destination Port: 53
Length: 50

Checksum: 0x604d [unverified]
[Checksum Status: Unverified]
[Stream index: 85]

Domain Name System (query)
Transaction ID: 0x475a
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.povertyactionlab.org: type A, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

[Response In: 1585]

No.	Time	Source	Destination	Protocol	Length	Info
1585	2018-10-17 16:36:37.004317	202.117.112.3	10.173.88.157	DNS	262	Standard query response

0x475a A www.povertyactionlab.org A 104.25.200.17 A 104.25.201.17 NS c0.org.afiliias-nst.info NS a2.org.afiliias-nst.info NS b2.org.afiliias-nst.org NS b0.org.afiliias-nst.org NS a0.org.afiliias-nst.info NS d0.org.afiliias-nst.org

Frame 1585: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.004317000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.004317000 seconds
[Time delta from previous captured frame: 0.000950000 seconds]
[Time delta from previous displayed frame: 0.000950000 seconds]
[Time since reference or first frame: 6.760850000 seconds]
Frame Number: 1585
Frame Length: 262 bytes (2096 bits)
Capture Length: 262 bytes (2096 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 242

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 240
Identification: 0x5228 (21032)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60
Protocol: UDP (17)
Header checksum: 0x8e12 [validation disabled]
[Header checksum status: Unverified]
Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 64019
Source Port: 53
Destination Port: 64019
Length: 220
Checksum: 0xa3e8 [unverified]
[Checksum Status: Unverified]
[Stream index: 85]
Domain Name System (response)
Transaction ID: 0x475a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0... = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 0
Queries
www.povertyactionlab.org: type A, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.povertyactionlab.org: type A, class IN, addr 104.25.200.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.200.17
www.povertyactionlab.org: type A, class IN, addr 104.25.201.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.201.17
Authoritative nameservers
org: type NS, class IN, ns c0.org.afiliias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 25
Name Server: c0.org.afiliias-nst.info
org: type NS, class IN, ns a2.org.afiliias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: a2.org.afiliias-nst.info
org: type NS, class IN, ns b2.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 21
Name Server: b2.org.afiliias-nst.org
org: type NS, class IN, ns b0.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: b0.org.afilias-nst.org
org: type NS, class IN, ns a0.org.afilias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: a0.org.afilias-nst.info
org: type NS, class IN, ns d0.org.afilias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169196
Data length: 5
Name Server: d0.org.afilias-nst.org
[Request In: 1584]
[Time: 0.000950000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1587	2018-10-17 16:36:37.006357	10.173.88.157	202.117.112.3	DNS	92	Standard query 0xb7e4

AAAA www.povertyactionlab.org
Frame 1587: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.006357000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.006357000 seconds
[Time delta from previous captured frame: 0.000514000 seconds]
[Time delta from previous displayed frame: 0.002040000 seconds]
[Time since reference or first frame: 6.762890000 seconds]
Frame Number: 1587
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 202.117.112.3
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 70
Identification: 0x3802 (14338)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
.0 0000 0000 0000 = Fragment offset: 0
Time to live: 64
Protocol: UDP (17)
Header checksum: 0xa4e2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157

Destination: 202.117.112.3
User Datagram Protocol, Src Port: 53408, Dst Port: 53
Source Port: 53408
Destination Port: 53
Length: 50
Checksum: 0x191b [unverified]
[Checksum Status: Unverified]
[Stream index: 86]
Domain Name System (query)
Transaction ID: 0xb7e4
Flags: 0x0100 Standard query
0.... = Response: Message is a query
.000 0.... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.povertyactionlab.org: type AAAA, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1601]
No. Time Source Destination Protocol Length Info
1588 2018-10-17 16:36:37.006539 218.30.19.40 10.173.88.157 DNS 124 Standard query response
0xf47a A www.povertyactionlab.org A 104.25.200.17 A 104.25.201.17
Frame 1588: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.006539000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.006539000 seconds
[Time delta from previous captured frame: 0.000182000 seconds]
[Time delta from previous displayed frame: 0.000182000 seconds]
[Time since reference or first frame: 6.763072000 seconds]
Frame Number: 1588
Frame Length: 124 bytes (992 bits)
Capture Length: 124 bytes (992 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 104
Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 102
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment

0... = Reserved bit: Not set
.1.. = Don't fragment: Set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0f6 [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157

User Datagram Protocol, Src Port: 53, Dst Port: 53648
Source Port: 53
Destination Port: 53648
Length: 82
Checksum: 0xc44b [unverified]
[Checksum Status: Unverified]
[Stream index: 77]

Domain Name System (response)
Transaction ID: 0xf47a
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0. = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1.... = Recursion available: Server can do recursive queries
....0. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
www.povertyactionlab.org: type A, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers
www.povertyactionlab.org: type A, class IN, addr 104.25.200.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.200.17
www.povertyactionlab.org: type A, class IN, addr 104.25.201.17
Name: www.povertyactionlab.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300
Data length: 4
Address: 104.25.201.17

[Request In: 1561]
[Time: 0.662183000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1589	2018-10-17 16:36:37.044923	10.173.88.157	218.30.19.40	DNS	92	Standard query 0xb7e4

AAAA www.povertyactionlab.org
Frame 1589: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.044923000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.044923000 seconds
[Time delta from previous captured frame: 0.038384000 seconds]
[Time delta from previous displayed frame: 0.038384000 seconds]
[Time since reference or first frame: 6.801456000 seconds]
Frame Number: 1589
Frame Length: 92 bytes (736 bits)
Capture Length: 92 bytes (736 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

Ethernet II, Src: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0), Dst: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Destination: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Source: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
.... .0. = LG bit: Globally unique address (factory default)
.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session
0001 = Version: 1
.... 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 72

Point-to-Point Protocol
Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 10.173.88.157, Dst: 218.30.19.40
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 70
Identification: 0x628a (25226)
Flags: 0x0000
0... = Reserved bit: Not set
.0... = Don't fragment: Not set
.0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0

Time to live: 64
Protocol: UDP (17)
Header checksum: 0xc78c [validation disabled]
[Header checksum status: Unverified]
Source: 10.173.88.157
Destination: 218.30.19.40

User Datagram Protocol, Src Port: 53408, Dst Port: 53
Source Port: 53408
Destination Port: 53
Length: 50
Checksum: 0x664d [unverified]
[Checksum Status: Unverified]
[Stream index: 87]

Domain Name System (query)
Transaction ID: 0xb7e4
Flags: 0x0100 Standard query
0... = Response: Message is a query
.000 0... = Opcode: Standard query (0)
.... .0. = Truncated: Message is not truncated
.... ..1 = Recursion desired: Do query recursively
....0.. = Z: reserved (0)
....0 = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.povertyactionlab.org: type AAAA, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1592]

No.	Time	Source	Destination	Protocol	Length	Info
1592	2018-10-17 16:36:37.220456	218.30.19.40	10.173.88.157	DNS	148	Standard query response

0xb7e4 AAAA www.povertyactionlab.org AAAA 2606:4700:20::6819:c811 AAAA 2606:4700:20::6819:c911
Frame 1592: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})
Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 17, 2018 16:36:37.220456000 中国标准时间
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1539765397.220456000 seconds

[Time delta from previous captured frame: 0.106945000 seconds]
[Time delta from previous displayed frame: 0.175533000 seconds]
[Time since reference or first frame: 6.976989000 seconds]
Frame Number: 1592
Frame Length: 148 bytes (1184 bits)
Capture Length: 148 bytes (1184 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)
 0 = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)
 0 = LG bit: Globally unique address (factory default)
 0 = IG bit: Individual address (unicast)
Type: PPPoE Session (0x8864)
PPP-over-Ethernet Session
 0001 = Version: 1
 0001 = Type: 1
Code: Session Data (0x00)
Session ID: 0x629d
Payload Length: 128
Point-to-Point Protocol
 Protocol: Internet Protocol version 4 (0x0021)
Internet Protocol Version 4, Src: 218.30.19.40, Dst: 10.173.88.157
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0000 00.. = Differentiated Services Codepoint: Default (0)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 126
Identification: 0x0000 (0)
Flags: 0x4000, Don't fragment
 0... = Reserved bit: Not set
 .1.. = Don't fragment: Set
 ..0. = More fragments: Not set
 ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 57
Protocol: UDP (17)
Header checksum: 0xf0de [validation disabled]
[Header checksum status: Unverified]
Source: 218.30.19.40
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 53408
Source Port: 53
Destination Port: 53408
Length: 106
Checksum: 0x26ec [unverified]
[Checksum Status: Unverified]
[Stream index: 87]
Domain Name System (response)
 Transaction ID: 0xb7e4
Flags: 0x8180 Standard query response, No error
 1.... = Response: Message is a response
 .000 0... = Opcode: Standard query (0)
 0.. = Authoritative: Server is not an authority for domain
 0. = Truncated: Message is not truncated
 1 = Recursion desired: Do query recursively
 1... = Recursion available: Server can do recursive queries
 0.. = Z: reserved (0)
 0. = Answer authenticated: Answer/authority portion was not authenticated by the server
 0 = Non-authenticated data: Unacceptable
 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
 www.povertyactionlab.org: type AAAA, class IN
 Name: www.povertyactionlab.org
 [Name Length: 24]
 [Label Count: 3]

Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)

Answers

www.povertyactionlab.org: type AAAA, class IN, addr 2606:4700:20::6819:c811

Name: www.povertyactionlab.org

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 300

Data length: 16

AAAA Address: 2606:4700:20::6819:c811

www.povertyactionlab.org: type AAAA, class IN, addr 2606:4700:20::6819:c911

Name: www.povertyactionlab.org

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 300

Data length: 16

AAAA Address: 2606:4700:20::6819:c911

[Request In: 1589]

[Time: 0.175533000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
1601	2018-10-17 16:36:37.696115	202.117.112.3	10.173.88.157	DNS	286	Standard query response
0xb7e4	AAAA www.povertyactionlab.org	AAAA 2606:4700:20::6819:c911	AAAA 2606:4700:20::6819:c811	NS d0.org.afilias-nst.org	NS	b0.org.afilias-nst.org NS a2.org.afilias-nst.info NS c0.org.afilias-nst.info NS a0.org.afilias-nst.info NS b2.org.afilias-nst.org

Frame 1601: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0

Interface id: 0 (\Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6})

Interface name: \Device\NPF_{5D52E7A2-EE68-4250-BF9F-5249138CADE6}

Encapsulation type: Ethernet (1)

Arrival Time: Oct 17, 2018 16:36:37.696115000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1539765397.696115000 seconds

[Time delta from previous captured frame: 0.107248000 seconds]

[Time delta from previous displayed frame: 0.475659000 seconds]

[Time since reference or first frame: 7.452648000 seconds]

Frame Number: 1601

Frame Length: 286 bytes (2288 bits)

Capture Length: 286 bytes (2288 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:pppoes:ppp:ip:udp:dns]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf), Dst: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Destination: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

Address: AsustekC_e2:8a:f0 (34:97:f6:e2:8a:f0)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Source: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

Address: HuaweiTe_3e:8f:cf (94:db:da:3e:8f:cf)

.... .0. = LG bit: Globally unique address (factory default)

.... .0. = IG bit: Individual address (unicast)

Type: PPPoE Session (0x8864)

PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x629d

Payload Length: 266

Point-to-Point Protocol

Protocol: Internet Protocol version 4 (0x0021)

Internet Protocol Version 4, Src: 202.117.112.3, Dst: 10.173.88.157

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)

Total Length: 264

Identification: 0x5229 (21033)

Flags: 0x0000

0... = Reserved bit: Not set

.0... = Don't fragment: Not set

..0. = More fragments: Not set

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 60

Protocol: UDP (17)

Header checksum: 0x8df9 [validation disabled]

[Header checksum status: Unverified]

Source: 202.117.112.3
Destination: 10.173.88.157
User Datagram Protocol, Src Port: 53, Dst Port: 53408
Source Port: 53
Destination Port: 53408
Length: 244
Checksum: 0x3ae0 [unverified]
[Checksum Status: Unverified]
[Stream index: 86]
Domain Name System (response)
Transaction ID: 0xb7e4
Flags: 0x8180 Standard query response, No error
1.... = Response: Message is a response
.000 0.... = Opcode: Standard query (0)
.... .0... = Authoritative: Server is not an authority for domain
.... ..0. = Truncated: Message is not truncated
.... ...1 = Recursion desired: Do query recursively
.... 1... = Recursion available: Server can do recursive queries
....0.. = Z: reserved (0)
....0. = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 0
Queries
www.povertyactionlab.org: type AAAA, class IN
Name: www.povertyactionlab.org
[Name Length: 24]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
www.povertyactionlab.org: type AAAA, class IN, addr 2606:4700:20::6819:c911
Name: www.povertyactionlab.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2606:4700:20::6819:c911
www.povertyactionlab.org: type AAAA, class IN, addr 2606:4700:20::6819:c811
Name: www.povertyactionlab.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 300
Data length: 16
AAAA Address: 2606:4700:20::6819:c811
Authoritative nameservers
org: type NS, class IN, ns d0.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169195
Data length: 21
Name Server: d0.org.afiliias-nst.org
org: type NS, class IN, ns b0.org.afiliias-nst.org
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169195
Data length: 5
Name Server: b0.org.afiliias-nst.org
org: type NS, class IN, ns a2.org.afiliias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169195
Data length: 25
Name Server: a2.org.afiliias-nst.info
org: type NS, class IN, ns c0.org.afiliias-nst.info
Name: org
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 169195
Data length: 5
Name Server: c0.org.afiliias-nst.info

```
org: type NS, class IN, ns a0.org.afilias-nst.info
  Name: org
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169195
  Data length: 5
  Name Server: a0.org.afilias-nst.info
org: type NS, class IN, ns b2.org.afilias-nst.org
  Name: org
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 169195
  Data length: 5
  Name Server: b2.org.afilias-nst.org
[Request In: 1587]
[Time: 0.689758000 seconds]
```