

**Joint Committee of the Higher Education
And Entertainment Communities
Technology Task Force**

BAYTSP'S RESPONSE TO

Request for Information

**Technologies for Addressing Issues
Associated with Unauthorized File Sharing
on the University and College Campus**

15 JUNE 2008

Contents

1	Introduction.....	3
2	Submission Requirements.....	3
2.1	Features of the Technology	3
2.1.1	<i>Network architecture.....</i>	4
2.1.2	<i>Scalability.....</i>	5
2.1.3	<i>Protocol identification.....</i>	5
2.1.4	<i>Granularity of protocols.....</i>	5
2.1.5	<i>Product Configuration and Installation.....</i>	6
2.1.6	<i>Content identification.....</i>	6
2.1.7	<i>Examination of network packets or file content.....</i>	7
2.1.8	<i>Distribution systems</i>	7
2.1.9	<i>Resilience of the technology to countermeasures</i>	8
2.1.10	<i>Testing and installed base.....</i>	8
2.1.11	<i>Competitive approaches</i>	9
2.1.12	<i>Third-party components.....</i>	9
2.1.13	<i>Comparison with Hypothetical Scenario</i>	9
2.2	Performance with respect to the Requirements Described in the 2007 Workshop Report 10	
2.2.1	<i>Identifying Infringing Traffic at the Campus Border.....</i>	10
2.2.2	<i>Responding to Infringing Traffic at the Campus Border</i>	10
2.2.3	<i>Identifying Infringing Traffic Local to the Campus Network.....</i>	11
2.2.4	<i>Responding to Infringing Traffic Local to the Campus Network.....</i>	11
2.2.5	<i>Supporting the Campus Judicial System</i>	11
2.2.6	<i>Considerations for Purchase and Operations.....</i>	12
2.3	Intellectual Property	12
2.4	Corporate Characteristics and Resources	13
2.5	Pilot Testing.....	13
2.6	Commercial Terms	13
2.7	Additional Information.....	14
3	Confidentiality.....	14

4	Conflicts of Interest	14
5	Readership and Dissemination	14
6	Miscellaneous	15
	6.1 No Obligations.....	15
	6.2 Neutrality.....	15

1 Introduction

BayTSP is a technology company that provides online copyright tracking and enforcement solutions. The technology searches for digital content on the major p2p protocols and IRC, UseNet, and Web 2.0 sites. BayTSP is engaged by the largest content owners, software companies, gaming publishers, music labels, and electronic book publishers in the world.

Because BayTSP is tracking on a variety of content from the largest content owners, software publishers and other digital content, BayTSP is the only online monitoring company that can provide organizations a complete view of activity of file-sharing activity on the networks.

BayTSP can be deployed externally to monitor targeted networks and the trading of copyrighted content.

2 Submission Requirements

This section outlines the structure within which technology vendors are invited to respond to this RFI.

This structure is intended as a guideline. If the vendor feels their submission can be better handled in another form, we still welcome their submission, although 1) it must respond directly to all the questions raised in the RFI, and 2) extensive variations in format may severely limit the effectiveness of the response for the reader.

2.1 Features of the Technology

This section of the response to the RFI should provide sufficient information about the vendor’s technology so that the reader can acquire an adequate understanding of the tool, its method of operation, and its capabilities and effectiveness.

All technology submittals that are considered by the vendor to be applicable to the problem addressed by this RFI will be considered. However, the Joint Committee of the Higher Education and Entertainment Communities believes that most proposals will range over the following classes of tools. Some submissions may include features of several of these classes of tools. In those cases where the vendor possesses multiple tools, each should be separately discussed in its particular area of class of tool.

Audit Tools - This class of tool covers applications that could be used by systems administrators to configure and maintain computer assets owned by the university or college. Such tools may allow auditing of installed applications against a standard “build” for the machine or may allow profiling of file archives on university-owned storage devices, for instance on public ftp servers, etc.

Bandwidth Shaping – This class of tools has the capability to adjust and/or alert other devices to adjust the amount of bandwidth and/or priority allocated in a network to a particular file type or application at any point in time. The technology may address uploading, downloading, or both, and may take origin or destination IP addresses into account.

Data/File Sharing Blocking – This class of tool takes an active role in blocking and preventing access to file-sharing and/or streaming applications on a network or machine basis. The technology may block access based on external information such as DMCA notices.

Matching, Screening and Filtering – This class of tool can match transmitted data with, for example, data in a predetermined database and provide administrative reporting and/or selective filtering. This includes technologies that can provide activity reporting without blocking.

User Management and Communication – This class of tool can match the inappropriate action with the infringer and then communicate with the user. This includes technology to configure graduated levels of response and actions.

Network Performance – This class of tool is directed at overall network operation, performance and traffic analysis. Such tools may simply provide information such as traffic data/session, source address, application type, destination address, ports, etc.

BAYTSP RESPONSE

The BayTSP technology falls under the category: Matching, Screening and Filtering.

BayTSP offers a range of products from a “lights-out/hands-free” fully hosted ASP model. BayTSP servers scan the Internet 24x7 for IP infringement activity for its clients and report the results of the ongoing protection through a client control panel.

2.1.1 Network architecture

The vendor should provide descriptions of how its technology could be installed in typical networks including architecture diagrams.

BAYTSP RESPONSE

The BayTSP technology monitors for content for a network outside of the network. Based IP address matching, BayTSP can provide and XML-

based reporting to the ISP/EDU Organization in near real time of activities on the network that may infringe on copyrights. This type of monitoring and reporting has already been implemented at non of the largest U.S. ISPs.

2.1.2 Scalability

Due to the high capacity of many university networks, particular reference should be made to the scalability of the tool. Each vendor should discuss the throughput of its technology (using aggregate bandwidth handled as the standard of measure), and the potential effects of its technology on network latency.

BAYTSP RESPONSE

The system is highly scalable. BayTSP states that they identify and document over 20+ million intellectual property infringements each day. Their patent pending technology can be used to track digital files on the Internet, including within peer-to-peer networks, Usenet news groups, IRC channels, File Transfer Protocol (FTP) servers, World Wide Web sites, and ,auctions sites.

Additional tracking and monitoring hardware can be added to achieve desired coverage up to full network coverage.

2.1.3 Protocol identification

The vendors should discuss whether and how network protocols are identified (e.g. by port number, by layer 7 analysis, etc.) and the methods that the vendor uses to update its software to detect new and mutated protocols. The vendor should address how the technology is able to adapt to changes in protocols as they evolve.

BAYSTSP RESPONSE

BayTSP continually (24x7x365) monitors and tracks all the actual ports and protocols used by the various P2P applications through its digital tracking system. As additional protocols and networks mature and gain critical mass, BayTSP develops the tools necessary to track the illegal IP activity on these networks as well.

2.1.4 Granularity of protocols

Each vendor should discuss its technology (where applicable) in terms of addressing those file sharing applications that employ multiple protocols (e.g. control, searching, file transfer, etc). Descriptions should be provided as to: which protocols does the vendor's

technology detect; whether the technology can address each of these protocols independently; and whether different rate limits can be set for “search” vs. “file download.”

BAYTSP RESPONSE

BayTSP has developed tracking tools for the most highly trafficked areas for Internet piracy and currently supports the following protocols:

- Internet Relay Chat (IRC/DCC)
- FTP
- NNTP (Usenet/Newsgroups)
- Ares
- BitTorrent
- Fast Track (KaZaa, Grokster, iMesh, etc.)
- Gnutella/Gnutella2 (Morpheus, Limewire, etc.)
- Direct Connect
- eDonkey
- Winnie
- Share
- Perfect Dark
- HTTP (world wide web)
- HTTP Auction Sites (select spiders)

The BayTSP approach to tracking and monitoring does not attempt to differentiate between a “search” and a “download;” instead they monitor for “offered” files within the P2P networks.

2.1.5 Product Configuration and Installation

The vendor should describe how much downtime is required for installation and maintenance and what elements of the network are involved. The degree of network integration and integration with other products should be presented. The vendor should discuss if the technology requires initial setup by individual users or requires installation of any components on individual user PCs. Specify if there are other setup or maintenance actions at the user level.

BAYTSP RESPONSE

BayTSP’s solution does not require downtime to the network. The scanning and reporting is an external monitoring of potential infringement activity on the network.

2.1.6 Content identification

If the technology operates at the individual file level and is intended to selectively identify communications that represent potential infringements of copyright law, explain in detail how the technology will identify such content. The vendor should specify what categories of content can be identified (i.e. compressed audio files, video, images, etc). The vendor should list any external content databases that are required, and whether or not they are proprietary. The vendor should indicate what information, if any, is captured and reported for further analysis and actions.

BAYTSP RESPONSE

BayTSP systems have integrated watermark and audio/video fingerprint technology. This is an open platform for vendors providing this type of content identification technology. BayTSP has licensing agreements in place with several technology partners. The digital asset tracking system was also designed to support a multi-tier file matching process.

In addition, BayTSP also maintains a proprietary database of cataloged content.

2.1.7 Examination of network packets or file content

Each vendor should indicate any aspects of the use of its technology that requires the examination or “opening” of network packets or files of information in order to carry out the technology's work. The vendor should indicate which fields of the Internet packets and which components of corresponding files are used by the technology and in what way. The vendor should include not only the degree of content inspection that is required in order to make the technology work, but also the degree of inspection and logging that the technology is capable of performing (even if “turned off” by the user or system administrator).

BAYTSP RESPONSE

The BayTSP system has several levels of network and content examination levels.

The 3 primary levels which are all available are as follows:

Level 1 – Validating the IP address and content offered

Level 2 – Validating the IP address and content offered and application used

Level 3 - Validating the IP address and content offered and application used AND downloading and validating segments of the file downloaded directly from the end user.

2.1.8 Distribution systems

Each vendor's response should specifically list all file sharing protocols or networks for which the technology is effective. In addition, the vendor should list other distribution systems, such as FTP, IRC, Usenet, for which the technology is applicable.

BAYTSP RESPONSE

Ares
BitTorrent
Fast Track (KaZaa, Grokster, iMesh, etc.)
Gnutella/Gnutella2 (Morpheus, Limewire, etc.)
Direct Connect
eDonkey
HTTP (world wide web)
HTTP Auction Sites (select spiders)
Internet Relay Chat (IRC/DCC)
FTP
NNTP (Usenet/Newsgroups)

2.1.9 Resilience of the technology to countermeasures

Each response should indicate the technology's ability to resist:

- (i) Countermeasures by file sharing software, for example, file compression, data encryption, etc.
- (ii) Circumvention efforts by users (i.e. port tunneling, proxy servers, fragmented packets, etc).
- (iii) Denial-of-service or other attacks against components of the technology.

BAYTSP RESPONSE

File compression and data compression is not an issue. The material must be discoverable and if it is not, the traffic generated is at a minimum.

BayTSP claims that the only effective countermeasure to its technology would be to categorically identify all of the company's IP blocks. While it is possible that this identification could possibly occur, BayTSP has a distributed architecture and constantly rotating IP blocks/Internet presence.

2.1.10 Testing and installed base

Each vendor should provide descriptions of the extent of testing of its technology, particularly the testing procedures employed prior to releasing an updated version (e.g. an updated detector) and specific examples (where available) of how technology applies in

real-life situations. The vendor should describe the features, maturity, status, availability, and installed base of its technology for each version that is currently supported.

BAYTSP RESPONSE

Testing of BayTSP's services is minimal. The data collection is external of the network. BayTSP system is already set-up for data delivery with minimal configuration. As mentioned earlier, BayTSP is already transferring p2p activity to one of the largest US ISPs.

2.1.11 Competitive approaches

Each vendor should provide clear descriptions of how its technology compares to other known competitive approaches and the benefits of its technology over competitive approaches.

BAYTSP RESPONSE

The BayTSP system provides the least intrusive monitoring system for the network. By engaging with BayTSP, the network operator will direct access to the content owner.

2.1.12 Third-party components

Each response should describe any third-party components required by the technology that are not provided by the vendor, but necessary for implementation (i.e. content databases, etc).

BAYTSP RESPONSE

The only third party component of the system would be licensed content identification and content recognition technology such as watermarking and fingerprinting technologies. The technology is not used for all services.

2.1.13 Comparison with Hypothetical Scenario

Technology and its capabilities to respond to the hypothetical scenario should be discussed.

BAYTSP RESPONSE

There are multiple implementation scenarios for BayTSP services.

1. BayTSP can forward infringement information via XML. The organization will match the reported unauthorized file sharing to its internal user logs to identify users.
2. BayTSP can forward to external reporting service that can automatically redirect browsers of users on the network.

2.2 *Performance with respect to the Requirements Described in the 2007 Workshop Report*

Provided in this section is a brief summary of the requirements that were documented at the April 2007 Workshop. Each vendor should refer to the report itself (<http://www.educause.edu/ir/library/pdf/CSD5170.pdf>) for a more detailed presentation. The vendor should provide a description on how their technology responds to the requirements presented in each of the areas in the Workshop Report.

2.2.1 *Identifying Infringing Traffic at the Campus Border*

The level of false positives (i.e., transmissions that are identified as infringing but are not) should be controllable by each individual campus. The settings that determine how many, or how few, false positives are generated should be selectable, rather than hard-wired into the solution. The solution should be time synchronized with the campus network to support accurate identification of the current assignment of IP addresses. The system should have a method for dealing with false positives (such as some sort of adjudicatory process that could be initiated by the student in response to an infringement notification). Further, it must be able to guarantee that critical traffic (e.g., network control signals) will always pass through the system unhindered.

The solution must be network friendly to the existing campus network architecture and “fail open.” That is, it must have no effect on network traffic in the case of system failure. The solution must be transparent to unrecognized traffic and induce no additional latency and jitter. The solution should operate in a way that leaves decisions to notify users and the Network Operations Center (NOC) of flagged infringements up to the individual campus. It should have the capability and flexibility to identify and/or block at either the application level or at the individual media file content level.

The solution must be able to evolve technologically as new protocols, signatures, modalities, and other changes occur in the file sharing technologies. Updates and upgrades should be supplied automatically by the vendor and must be easy to install and operate. The solution should work not only at the current speed, but also have the ability to be upgraded through a range of speeds (E.g. 1-10-100 Gigabits/sec) in tandem with the campus network.

Logging should be capable of being turned on or off, as well as be able to set the retention and deletion dates of logs, determine what is captured in the logs, and how those logs are used. The ability to move logs to other devices should also be a capability, and such logs should be protected.

BAYTSP RESPONSE

The BayTSP solution is a passive external solution that does not directly impact the network. System updates are implemented seamlessly.

Several controls are in place to eliminate false positive detections.

2.2.2 *Responding to Infringing Traffic at the Campus Border*

The technology should be selectively configurable to perform a range of responses, and the response policy at the campus level should be capable of being modified according to such considerations as source, destination, etc. The solution should be capable of integration with existing judicial systems so that the campus could elect to have an automated response to those users committing infringement violations. A flexible white list of addresses that will never be blocked should accompany a solution that blocks at the border.

BAYTSP RESPONSE

The BayTSP system can be configured other reporting systems.

2.2.3 Identifying Infringing Traffic Local to the Campus Network

Technology solutions should be capable of identifying infringing traffic within subnets at the lowest possible level. Technology implemented on the internal network must meet all the network-friendly requirements discussed in the border case in 6.2.1.

BAYTSP RESPONSE

The BayTSP solution is a passive external solution that does not directly impact the network.

2.2.4 Responding to Infringing Traffic Local to the Campus Network

Technology implemented must support the usual topologies of internal campus network architecture. The technology cannot require routing all traffic through single points of failure. The overall solution must not interfere with the legal access to and transport of, non-infringing or authorized content within the campus network. The technology should provide the ability to select different levels of responses to flagged infringements. A technology designed to identify infringing traffic local to the net should support multiple CIDR blocks, or IP address blocks.

BAYTSP RESPONSE

The BayTSP solution is a passive external solution that does not directly impact the network.

2.2.5 Supporting the Campus Judicial System

Technology should provide appropriate, integrated, automated support for the campus judicial system and an interface for reporting flagged infringements. Communication between the identifying technology and the network operators (judicial system) should be

secure. The technology should be flexible enough to provide campuses with a broad range of metadata and allow each campus to select what information is required. Communication of evidence to and from campus systems should be tamper-proof.

BAYTSP RESPONSE

The BayTSP system can be configured other reporting systems.

Avoiding Disruption of All Non-infringing Traffic

Technology should not affect the transmission of any and all non-infringing traffic. It should have the ability to support access to and distribution of content that has been flagged as potentially infringing, but could be permissible under fair use.

BAYTSP RESPONSE

The BayTSP solution is a passive external solution that does not directly impact the network. BayTSP system does not impact any transmissions directly.

2.2.6 Considerations for Purchase and Operations

The technology should possess the characteristics of predictability, transparency, auditability, and scalability. Pricing must be predictable and include cost to purchase (or license), install, operate, maintain and upgrade.

BAYTSP RESPONSE

The BayTSP system is transparent and scalable. The service is a monthly subscription.

2.3 Intellectual Property

This section of the vendor's response to the RFI should provide information concerning intellectual property associated with the technology. The information should provide insight as to whether any patents have been applied for, when and in what territories, and what (if any) claims have been granted. Where a patent has been granted, the vendor should provide the patent number and attach an abstract of the patent.

The vendor should remember that submissions to this RFI are governed by Section 7. The vendor should not have the expectation that information held to be confidential will necessarily remain within the Joint Committee. **(Confidential information should not be included in the response.)**

BAYTSP RESPONSE

BayTSP has several patent applications for content identification and tracking and content management database.

2.4 Corporate Characteristics and Resources

This section of the vendor's response to the RFI should provide information about the vendor's corporate capabilities. Include information about the vendor in terms of general and specific corporate characteristics: size, personnel, facilities, year of organization, corporate history, clients, revenues, capitalization, investors, etc. Information about corporate products or technologies other than that directly applicable to this RFI should not be included.

BAYTSP RESPONSE

BayTSP is a privately held company founded 1999. BayTSP is head quartered in Los Gatos with offices in Utah and Iowa. Additional offices will be opened in the UK and Japan. Data Centers located in the US, China, UK, and Japan.

The clients include all of the major US media companies, software, video games and record labels, and book publishers.

2.5 Pilot Testing

It is possible that certain colleges or universities may elect to test some of the technologies. The selection of those technologies will be done by the individual campuses based in part upon the results of the knowledge base created as a result of this RFI. Many factors will enter into the decision as to which technologies will be tested. One significant factor will be the level of interest and potential involvement of the vendor in the actual testing. Therefore, the vendor should present the vendor's concept for testing its technology in a real-life situation on campus. The vendor should also provide its concept for an evaluation license and any conditions that are associated with it.

The vendor's schedule for implementing its particular technology should be provided, allowing a period of sufficient duration to test and evaluate the results of that implementation.

The vendor should also provide information regarding the costs that might be incurred by a campus during pilot testing as well as information on whether or not they might consider conducting testing on a pro bono basis.

BAYTSP RESPONSE

BayTSP is willing to share a static report to the University upon request.

2.6 Commercial Terms

This section of the vendor's response to the RFI should discuss, in general, information about the commercial terms for its product (e.g. requirements for an annual license,

requirements for annual maintenance, ability for one-time purchase). In those cases where the vendor has published prices for the subject technology, the vendor should provide those prices. If standard licenses exist, they should be provided as well. **In no instance should the vendor provide cost information that would not be considered public information.**

BAYTSP RESPONSE

BayTSP will provide pricing information upon request.

2.7 Additional Information

This section of the vendor's response should present other information or raise issues that the vendor considers important in terms of documenting its product.

BAYTSP RESPONSE

3 Confidentiality

This RFI solicits detailed information including information about the vendor's intellectual property. The vendor, in response to this RFI, **should not provide information that requires the protection of a nondisclosure agreement.**

It is anticipated that an understanding of the capabilities of vendor technologies, gleaned from the response to this RFI, will be communicated to organizations affiliated with the Joint Committee of the Higher Education and Entertainment Communities. The vendors may or may not be given the opportunity to review and comment upon the documentation of **its individual technologies** prior to the release of such documentation, so the vendors' response to this RFI should be as complete as possible. Material that is considered proprietary or confidential can be referred to, but not included in the vendor's response to this RFI.

4 Conflicts of Interest

The vendor should disclose any potential or existing conflict of interest that it may have in either its response to this RFI or in the conduct of pilot testing at campuses that elect to participate in such tests. Conflicts of interest should also be noted with respect to any other products or services that may be required in order to deploy the vendor's technology for this project.

5 Readership and Dissemination

The results of documenting the responses to this RFI will be reported by the Technology Task Force to the Joint Committee of the Higher Education and Entertainment Communities. The committee will share the information more widely in the form of a

knowledge base. **It cannot be guaranteed that the information in the knowledge base concerning the technology responses to this RFI will be limited to those parties.**

6 Miscellaneous

6.1 No Obligations

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities reserves the right to cancel this RFI at any time. Technologies may or may not be selected for pilot or evaluation testing at the discretion of individual campuses.

6.2 Neutrality

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities will neither recommend nor approve any response to this RFI. The task force will not endorse specific business models or technologies. Evaluation and testing that may be conducted by individual campuses of selected technologies will in no way indicate a preference for any technology or vendor over another competing technology or vendor.