



Escalated Response System Testing utilizing Audible Magic and Introducing Birdtrax to the Campus Community

Executive Summary

Capitalizing on Illinois State's extensive background and experience within the area of digital downloading, the University undertook a "real world" production test of the network appliance CopySense from Audible Magic. Of interest was the signature detecting technology of copyrighted media (music, movies, etc.) along with the framework to establish an educational and judicially-based escalated response system. Simultaneously, the University mounted a 'launch website' titled BirdTrax and accompanying marketing campaign to promote legal media alternatives. By the end of the test, it was judged Audible Magic was performing reasonably well. But the test was shortened to several weeks due to the amount of time used in customization, local web programming, and software bug fixing. Due to the difficulties in deployment during this constrained period and the inability to scale the test widely, the results were incomplete. For these reasons, in addition to legal concerns of privacy and the proposed financial value proposition, it was decided that the product in its tested form would not be used at Illinois State for an escalated response system. BirdTrax, however, was deemed crucial and was reviewed, expanded, and promoted for the Fall 2008 semester.

Part A – Escalated Response System Testing utilizing Audible Magic

Note: Illinois State partnered with the company Audible Magic for this test utilizing their product, the CopySense Network Appliance which is a hardware/software package. Unless specified, the terms Audible Magic, CopySense, and appliance are used interchangeably to describe this product throughout this document.

Background

Among the reasons for starting the Digital Citizen Project at Illinois State, leaders were responding to the overwhelming task of processing an avalanche of DMCA notices. It was through Illinois State's DMCA processes in 2005 that administrators were time-challenged but more alarming, students were receiving "boilerplate letters" that didn't do a good job of turning a 'wrong' into an educational experience. We were looking for a way that technology could proactively and extremely reliably determine illegal file sharing (while letting legal peer to peer proceed) and then help students understand the illegal nature of such activities. We restricted our scope to the residence halls which use a direct wired Internet connection (no wireless access exists in student rooms). In talking with vendors, two stood out. Red Lambda had technology which provided a framework for interacting with students which emphasized a tiered approach whereby increased infractions led to increased actions. Audible Magic had technology which could identify on a signature basis copyrighted files (much like an anti-virus company identifies an exact virus) through the use of hash numbers or digital fingerprinting. After suggesting for some time, quite seriously, that the two companies should work together and meld their products, Audible Magic indicated a willingness to work with us and code an "escalated response" portion of their product. The full timeline of the test can be found in Appendix A1.

Escalated Response Content Creation Committee

During the Fall 2006 semester, a committee was appointed to look at the issue and suggest what might be Illinois State's response if we could utilize or even develop such a system. The committee was comprised of half students and half staff. This composition turned out to be critical to our implementation as we were able to articulate Illinois State's values concerning illegally transferred media. And it forced us to develop a vision of what we wanted technology to help us implement before we even dealt with the technology specifics. The fact that students had a large role in this process can't be stressed enough as when it came time for implementation, we had good support—not unanimous by the entire student body, but certainly very positive from student leadership. It was also politically fortunate that one of the student committee members went on to be elected student body president the following year.

Another key component to this initial team was the role of our existing student judicial or conduct administrators. Referred to the office of Community Rights and Responsibilities on our campus, these leaders have been big proponents of extending the ethical standards of our campus to electronic environments. A system whereby the Information Technology community does discovery and initial notification but then turns over cases of repeated or serious events has worked well at Illinois State. The theories and practices which judicial staff were able to bring to our discussions were invaluable as they had the experience from many other problem areas such as alcoholism, classroom cheating, etc that have much longer historical records. Thus, we were able to look at this issue within a larger context and not 'just because it was in cyberspace' did new rules need to be written. This committee was disbanded in Spring 2007 with thanks for a job well done. Their outline of a desired technology system can be found in Appendix A2. Even though all the technology pieces didn't come along until a year later, it was the committee's framework which served as the roadmap.

Project Development

Audible Magic's CopySense appliance was already in use at Illinois State in a monitoring mode. It supported various research pieces of the Digital Citizen Project and was one of the prime instruments for data capture. A variety of local network engineers were supporting it in addition to support staff at Audible Magic. As development started on escalated response, we had one engineer and one web developer working directly with Audible Magic on a constant basis. New software versions would be released (what would be considered alpha and then eventually beta releases) and Illinois State would provide feedback and seek additional capability. We were aware of several other universities also working with the escalated response portion of the product although we never worked directly with them. Much time was spent on how information would be passed back and forth from the CopySense appliance. It was through this process that it became clear that the web hosting and front-end web pages (i.e., the web part which a student would actually see) were Illinois State's responsibility. This was in addition to the mechanical processes for communicating with various entities on campus. Audible Magic would provide the detection, a database to maintain a running count of infractions by IP address, and then a redirect structure for any http traffic. ISU would handle the rest. Other major work took place with our engineers as we structured our network bandwidth, IP subnets, and DHCP leases – no insignificant pieces to the project.

Testing Phase

Work progressed for much of Spring, Summer, and Fall 2007. An important milestone was on October 8, 2007 when we met with the Student Government Association executive team and staff and announced that we planned to implement the escalated response system in the residence halls, gradually, as our testing allowed. We received a green light to move forward with two caveats: 1) we clearly communicate with each student that would be affected before the system was implemented, and 2) we make a concerted effort to educate the student body about legal alternatives. Both were deemed proper and desirable by the project leaders. The text of the email eventually sent to effected students is in Appendix A3.

With help from campus project managers, we put together a three stage plan for testing escalated response before the system would be deemed ready to be rolled out to the entire campus:

1. Proof of concept to management team
2. Testing in a Quality Assurance lab
3. Release to one group of students (a networking subnet) followed by an expanding range of subnets

As with the development of many complex technical projects, it seemed that while much work was being done, actual progress and milestone achievements were slow. Obstacles kept coming up such as in late October when the campus moved its external bandwidth availability from 250Megabytes to 1 Gigabytes. This introduced various load issues with Audible Magic and necessitated a new box. Problems like this, even once identified, would take weeks to correct and added to the development time.

Establishing Levels

Utilizing the work of the escalated Response Creation Committee (Appendix A2) with follow-up input from student conduct staff, we arrived at a three level system for infractions. The first action of each level was that the student was placed in a 'timeout' with port 80, off-campus, Internet traffic (i.e. web access) redirected and contained to our instructional web site. Then specific steps were required first to serve as an educational response, then to remove the redirect, and finally to provide a cool down period. Screen shots of each can be found in Appendix A4-A6. Distinguishing characteristics of each level:

- Level One – 6 multi-choice questions concerning copyright, 15 minute timeout
- Level Two – 3 essay questions for the student to reflect on their moral actions, one day timeout, and a notice within student conduct record
- Level Three – Immediate referral to student conduct offices where case would become part of discipline process most likely resulting in a hearing and possible suspension.

Given the flexibility of CopySense in establishing points per infraction and threshold levels, we initially did not have a good what represented effective values. As this was an early implementation of Escalated Response, Audible Magic had little guidance in this area. For fear of overwhelming student support needs, we decided to put the levels high with the plan to reduce as we saw what happened—although we later learned that by changing threshold levels, all points to each IP were reset. Our beginning parameters were 1 point per signed upload or download with threshold levels of 50/100/200. We then reset everything to threshold levels of 20/40/80. Finally we increased to 2 points per signed upload or download. This seemed to be a good strategy for us in finding the most egregious file sharers without overwhelming support staff.

Activation and Results

The test started on April 15th with deployment in a single residence hall (Monroe House) consisting of 217 students. On April 28th we added 600 students in three additional halls. The test was extended to the last day of classes of the Spring semester, May 2nd, for a potential total of 18 days of operation. The first escalation did not happen until April 29th. At first, we attributed this to the effectiveness of the warning email sent to all affected students before turning on the CopySense appliance (still a possible contributing theory). But then an Audible Magic software bug was discovered that was resetting all points each day and thus making it difficult for a student to get escalated. This problem was fixed on Apr 28th leaving us only 5 days of full operation. The final tally for sanctions is as follows:

- 23 students reached the point where they were escalated to level 1.
- 20 of these students went through the tutorial and got out of level 1
- One of the students reached level 2 This student responded to questions and got out of level 2.
- No one reached level 3.
- Three students were still in escalation when the test run ended. The rest had completed the surveys.

We believe this was enough testing to verify that CopySense worked within the context of the test, but not enough to measure the long-term effectiveness.

Conclusions and Anecdotes

We hope that the work which we did can be utilized by others. For this reason, the following points are made in regard to our test. It has been noted that we upgraded our hardware and software several times. Our testing ended with the CopySense version 3.3 and our statements apply to that version.

By the end, it was judged that Audible Magic was performing reasonably well. But the test was shortened to several weeks first due to the heavy amount of time in customization, local web programming, and software bug fixing that occurred in getting ready for the test. Then the actual time with points accumulating (due to the software bug) was only a week.

Running a separate Audible Magic appliance in monitor mode was helpful both in terms of collecting data but also for debugging and problem solving. At the point we were running CopySense on one appliance and saw that no one was being escalated, we queried another CopySense box which was in

monitoring mode and it saw much higher activity. It took some time to realize that the escalated response box was resetting all values each day and not cumulating them.

What effect did the email notice have on piracy? This is a lingering question and deserves much more research. As the test was started and we sent out the warning email, it is our opinion that piracy was reduced. By how much we don't know. For how long would have this lasted with the email alone? To carry this idea further, what reduction in piracy would we see if we simply moved Audible Magic's appliance around the network (i.e. NOT have 100% coverage at all times but simply 'spot checks')? These and other questions are worth exploring.

Being an IP based system has challenges. All tracking in CopySense is done via a user's IP address. This necessitates that for the cumulative period being monitored, a user has the same IP if the desire is to be 100% comprehensive and inclusive. We have a single wired port-per-person model which utilizes DHCP leases in the residence halls set for 2 weeks (unlike wireless, for example, where the lease is 5 minutes to prevent DHCP scope depletion). The thinking is that the longest a student would be removed from their room was 10 days (i.e. the span of spring break). However, this presents risks as nothing prevents a student from either intentionally or unintentionally receiving a new DHCP address which would cause the points accumulation to be incorrect. Or in the situation where another student inherited a previously released IP address, the point totals for the new student would incorrectly have carried over from the previous student. For our campus, we were willing to let such slippage go as we did not think it would be a major problem and were satisfied at the less than 100% point coverage – but an enterprising student can easily outsmart the system. One of our requests to Audible Magic was to consider building a system based on Network Interface Card MAC address but that still wouldn't resolve a student with multiple computers. A system based on a person's unique University logon ID would be the closest to ideal, but that would require substantial changes both at Illinois State to have a common network sign-on and changes with CopySense so that it was aware and kept track of points via user ID.

Bandwidth and load capacities are still unknown. The escalated response appliance performed adequately up to our maximum test of 800 users. We ran out of time before we could expand this further, but we have concerns that a single CopySense appliance could handle our entire campus (6400 users) utilizing the escalated response functionality. This deserves further explanation of how we utilized CopySense. The escalated response box which had a 1GB/s interface was placed on the wide area network (WAN) which had a capacity of 1.179GB/s from two different ISPs. P2P traffic was shaped using a PacketShaper appliance to 28Mbps (14Mb/s on each of our WAN ISP links) and limited to the designated subnets for the 800 students in the test. Four observations:

- 1) Audible Magic staff could not give us an exact upper limit of load
- 2) We were told the most likely behavior exhibited at saturation would simply be dropped packets—something we may or may not be able to catch. Many times we closely reached points of saturation when running the CopySense appliance in monitor mode only on a campus-wide basis.
- 3) From a bandwidth perspective, CopySense was viewing the entire network (given it was located at the WAN) but our understanding is that the actual load has less to do with the raw amount of traffic and more to do with the restricted amount of traffic that is being examined. We did see an increased processor load factor when escalated response was added to the monitoring-only functions.
- 4) We are aware that multiple Audible Magic appliances can be utilized on a campus separated by subnet, but the database which holds points for escalated response functionality is local to each box and can't be shared (thus a student would have separate counts on each box).

Student outcry was mostly silent. We expected to hear much negative reaction and were even prepared for student newspaper editorials when we started performing the test. But such never came and the reaction was mostly silent. It could have been the time of the year (spring when the weather was turning nice, class papers and projects were due, etc). It could have been because of our efforts to communicate ahead of time.

It is important to communicate with all campus personnel who might have contact with effected students. We think we did a pretty good job of thinking through who might be contacted if a student had problems. It started with the University Computer Help Desk unit, the technicians that service students in their residence halls (ResNet), the telecommunications department, and student conduct personnel. Each of these needed to be able to query an individual student (i.e. via their IP address) to find if the Audible Magic system was the cause of any technical problems. Prior to deployment we were very nervous about an onslaught of support requests but then little developed. We continually queried each group and received replies such as this one from a Help Desk analyst “Per Dave's request, here's an update from the Help Desk on ER... <crickets chirping>” Even though there were no issues, we were glad everyone was on board.

The involvement of conduct staff up front was wise. We already had a strong relationship with our student conduct staff and they had experience with Internet issues. But their willingness to be a part of this new system and contribute with well established theories from their field made for a stronger solution. It was also revealing that most IT staff tended to be more lenient when it came time to create punishments. Judicial staff (and student leaders) were generally advocates for more severe punishments up front to get a student's attention so that future punishments were not needed.

During a network timeout, there should be a way to stop P2P traffic. As the system exists, when a user is in timeout, their http port 80 traffic is redirected. Note that this is for external traffic (off-campus) only and not on-campus. For us that worked well as students could still get to local academic resources (such as course systems, test servers, etc) but still be majorly inconvenienced. However, P2P traffic continues to be allowed in this timeout. This seems illogical that you would allow a student to continue their P2P activities – especially given the upload distribution nature of this activity. Audible Magic tried to respond to this issue, but could only provide a means in which a network flood was pointed toward the individual port to make it seemingly shutdown. This was a forbidden activity on our campus given our history with viral, malicious, and denial of service IP floods so was not implemented.

The product as tested is not an out of the box solution and requires substantial programming investment. Much custom programming would have to be done on any campus implementing escalated response. The good news is this allows a campus to tailor the product to their needs. However a campus should be ready to make this investment to receive basic data from CopySense APIs and utilize this in locally written web pages requiring, at minimum, a programmer's expertise. Also of note is the amount of information available via the APIs is limited. For example we wanted to get exact offending media title information to show to students and for capture in judicial records, but such was not available. Finally, we had to find a way to translate the student's IP address (how Audible Magic tracked) to an actual University ID for support and record processes. For our campus, this is a highly manual process so we wrote a self-identification system, which while not fool-proof, was the best we could do.

Changing points during a period can be problematic. Even during our short testing period, we decided it was necessary to change our points scheme. Doing so is easy, but we had to start all over with counters set at zero. Having the flexibility to customize point schema is nice, but be aware of this and think how you want points to accumulate.

We only relied on actual copyrighted signature and not metadata finds. The appliance has two ways of detecting material. The first is by actual signature which uses methods such as “hash” number identification or “digital fingerprinting” to match content against a known database. Based on our testing and experience, our confidence in signature matching grew over time to where we believe we had very few, if any, false positives. There is also another “level” which simply looks at metadata info. Based on our own research and discussions with others we elected not to utilize this as by nature, it is not as discriminate. Note that by using signatures only, music is well covered, but movies and television are weak per the amount of titles in the CopySense signature database.

Audible Magic offers good customer support. Through the testing, we felt that Audible Magic as a company and their individual technical support professionals responded well when we had needs.

Fall 2008 Environment

By the end of the test, it was judged Audible Magic was performing reasonably well in the limited environment which is described. However, we do not feel we had expanded the test to enough students to make a good determination of the system. While the vendor was responsive, we were making calls for information or tweaks throughout the entire process. We have unanswered concerns regarding scaling given the usage of a single database appliance that is not able to be load balanced. We also have capacity concerns of the appliance regarding bandwidth throughput when the escalated response components are running (we closely reached points of saturation when running in monitor mode only). With these factors in mind, it was decided not to continue with the Audible Magic Automated Escalated Response system for Fall 2008. Three additional factors went into this decision and should be discussed:

1. The CopySense appliance has options to identify pornographic material. The further identification of child pornography is unclear. While there exists an option to filter out such material, we could not be convinced that such information would not be collected and retained somewhere on Audible Magic boxes. This was information and a risk that Illinois State was not willing to take.
2. The second issue was a realization that even with this solution, we could not guarantee that its utilization would result in eliminating DMCA notices, litigation holds, subpoenas, or lawsuits for the campus.
3. The third issue regards cost. The cost/benefit proposition for Illinois State was not deemed favorable when considering the number of boxes potentially needed for our campus.

It should be noted that all constituencies at Illinois State were very happy with the escalated response concept – especially the automation. In fact, personnel from our student conduct area were disappointed when it was decided not to continue the program (even though it meant more work for them). We really favor this educational approach.

For the Fall 2008 semester, we are trying a new test which blocks all P2P in residence hall and wireless networks with exceptions granted based on request. This is being done with currently owned network intrusion devices with no additional expense. Stay tuned as we learn more and report about this experiment – the next one of many with the Digital Citizen Project.

Appendix A1

Integrated Timeline of Escalated Response and BirdTrax at Illinois State University

Note: Those items related to the BirdTrax marketing campaign with blue highlight

Date	Notes/Activity
Late 2006 – early 2007	Escalated Response Content Creation Committee meets to establish levels and strategy for each
Oct 8, 2007	Meeting with Student Government leaders
Feb 5, 2008	Proof of concept 1 testing in lab Comprised of Help desk, telecom, security, & project staff
Feb 18	Proof of concept 2 – lab Comprised of Students
Feb 26	Formal Debriefing meeting and all-staff check-in
Feb 29	Large Group Call with Audible Magic
Mar 3	Meeting with Judicial staff
Mar 4	Upgrade to AM appliance (3.3) resulting in an “increase in the identification rates on the machine” due to enhanced algorithms
Mar 10 to Mar 14	Spring Break Week
Mar 17 to Mar 23	1 st week of Birdtrax teaser slides on Residence hall cable TV information channel (Campus Connections). [Appendix B5 for content examples]
Mar 24 to Mar 30	2 nd week of Birdtrax teaser slides on Residence hall cable TV information channel (Campus Connections). [Appendix B5]
Apr 11	Final determination to go
Apr 14 to Apr 28	The first 2 of 6 Birdtrax Signcades strategically placed on plaza where approximately 8-10 K students/faculty pass each day. [Appendix B5]
Apr 14	100 posters were distributed throughout the campus buildings including all major classroom facilities, student center, bookstore, student center, library and immediate off-campus sites. [Appendix B6]
Apr 14	Notification email sent out to Monroe house, warning them that ER would be activated in their house shortly. [Appendix A3]
Apr 14	WZND 1 st Birdtrax 30 second radio teaser message, plays varies times during the week 4/14-4/20. Feedback from radio station contact was there was some buzz about the spot. [Appendix B7]
Apr 15 10:15am	ER brought online for Monroe house at 10:15AM with original Point system of 50/100/200 with 1 point given for each upload or download IP ranges - 10.23.13.0/24 and 10.23.14.0/24
Apr 18 12:00 noon	Points all reset and changed to 20/40/80
Apr 21	Bookmarks began to be distributed by Milner Library. Also at the Information Desk (main floor) and Barnes & Noble’s (2 nd floor) in the Bone Student Center. Continue to do this. [Appendix B8]
Apr 21 to Apr 25	3 rd week of Birdtrax teaser ran on Campus Connections interspersed with Milner Library marketing slides. This one included the Birdtrax website address. [Appendix B5]
Apr 21to Apr 27	WZND 2 nd Birdtrax 30 second radio message begins play. Runs various times during the week. No feedback received. Similar to first one in appendix B7.
Apr 22	Birdtrax insert is distributed with the student newspaper, Vidette. 8000 distributed around campus. [Appendix B9]
Apr 25	Consultation with AM regarding lack of escalations led to suspicion that there

	was a problem with the logging for the ER box.
Apr 25	Points per violation up to 2
Apr 25	Notification email sent out to Randolph, Clay, and Adams houses [same as Appendix 5] 653 students
Apr 28 12:30p	AM located and corrected a bug that was causing the ER unit to wipe the escalation table every night. The patch was pushed down to the ISU ER unit as soon as it was completed.
Apr 28 2:12p	ER expanded to Randolph, Clay and Adams houses. Point system remains 20/40/80 with 2 points per violation
Apr 28 to May 5	The second 2 Birdtrax Signcades strategically placed on plaza where approximately 8-10 K students/faculty pass each day. [Appendix B5]
Apr 29	First level one escalation detected. One hit ER at 00:02:00 this morning, the other at 01:42:01
May 1	First level 2 violation detected. Student claimed that she had removed the software, and was unfairly escalated. The system had detected traffic on her IP for two days <i>after</i> she claimed to have removed the software.
May 2 10:00am	ER test ended
May 5 to May 30	The third 2 Birdtrax Signcades strategically placed on plaza where approximately 8-10 K students/faculty pass each day. [Appendix B5]

Appendix A2

Summary of Escalated Response Content Creation Committee

Group work of 11/15/06

Three levels based on points and number of copyrighted signed songs.

LEVEL ONE - education

Six web steps The ISU Appropriate Use

Policy (link) also prohibits this activity.. For questions contact (whoever/whatever email).

1 – stop. Copyright violation. This is your first warning.

2 – You have attempted to download copyright-protected music. This is a violation of US Copyright Law (with link to pertinent section).

Here is the offending IP/title - [showing offending titles]

Please review this information

3- educational tutorial [Justin to develop]

US copyright law

ISU appropriate use – you have signed already

RIAA/MPAA campaigns to target college students (include video info)

P2P apps can open up your computer (link for removal instructions)

Legal Subscription services are available

4 – acknowledgement of info

Next consequences

Future attempts to illegally download music will lead to escalating penalties

List of helpful places (Univ Computer Help Desk, Resnet RCCs, TechZone)

Info on how long they will be out (expectations as to what is next)

Where to go while no outbound access (labs, etc)

[enter ULID/password]

5- cooling off period

[send email to ULID office repeating instructive info]

→ during cooling off period

6 – you in timeout – redo first screen

Contact info repeat

LEVEL TWO – ethical situation (why did you not change your actions based on first violation?)

1 – stop. Second warning

2 – the problem is once again... copyright issue

Here is the offending IP/title that got you to level 2 - [showing offending titles]

??? time for offending download titles

??? show time for level 1

You must review and respond to this information

3-- Ethics exercise – what does it mean to be a digital citizen

We are meaner

Why are we concerned about this

What is impact on you and University

5 screens [CRR to develop]

text box response of reflective questions

-- emailed to CRR along with ULID/Password

4 –

Next consequences

Future attempts to illegally download music will lead to no outbound Internet for rest of semester and other penalties

Info they will be out until questions in step 3 above reviewed.

(expectations as to what is next)

Where to go while no outbound access

5- cooling off period until cleared via CRR

[send email to ULID repeating instructive info]

→ ???can IWSS develop app for CRR to enter IP and clear student??

→ during cooling off period

6 – you in timeout – redo first screen

Contact to CRR for status. List hours.

LEVEL THREE

1 – you are in perm URL redirection & P2P block

Enter ULID, you will be contacted by CRR

→ ???can IWSS develop app for CRR to enter IP and clear student??

→– if contested case, CRR calls for a TNSS manual lookup for evidence

Appendix A3

Notification email sent to students before escalated response was turned on

To: list of students in Monroe House, Watterson Towers.
From: digitalcitizen@ilstu.edu

To curb piracy on campus, Illinois State University is proactively working with technology that is designed to identify copyrighted material being transmitted over peer-to-peer (P2P) networks.

Starting April 15, 2008, Illinois State University will begin monitoring P2P downloads. If you engage in copyright infringement by downloading copyrighted files without permission, you will be placed in the Escalation Response system.

There are three levels to the Escalation Response system, with each level resulting in escalating penalties. Continued downloading will lead to Escalation Response Level Three, and you will be required to undergo disciplinary review by the Community Rights & Responsibilities (CRR) office.

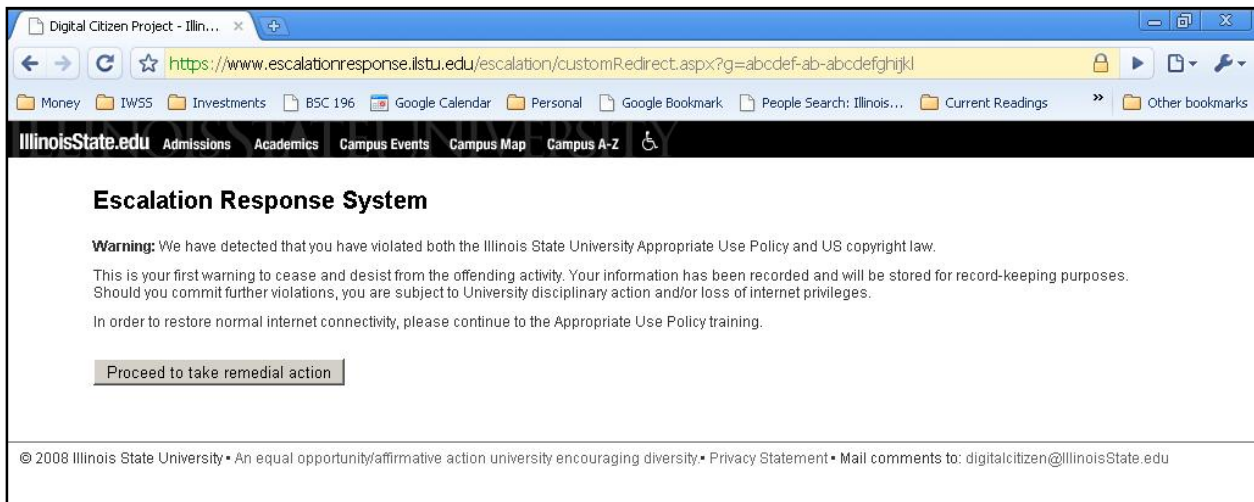
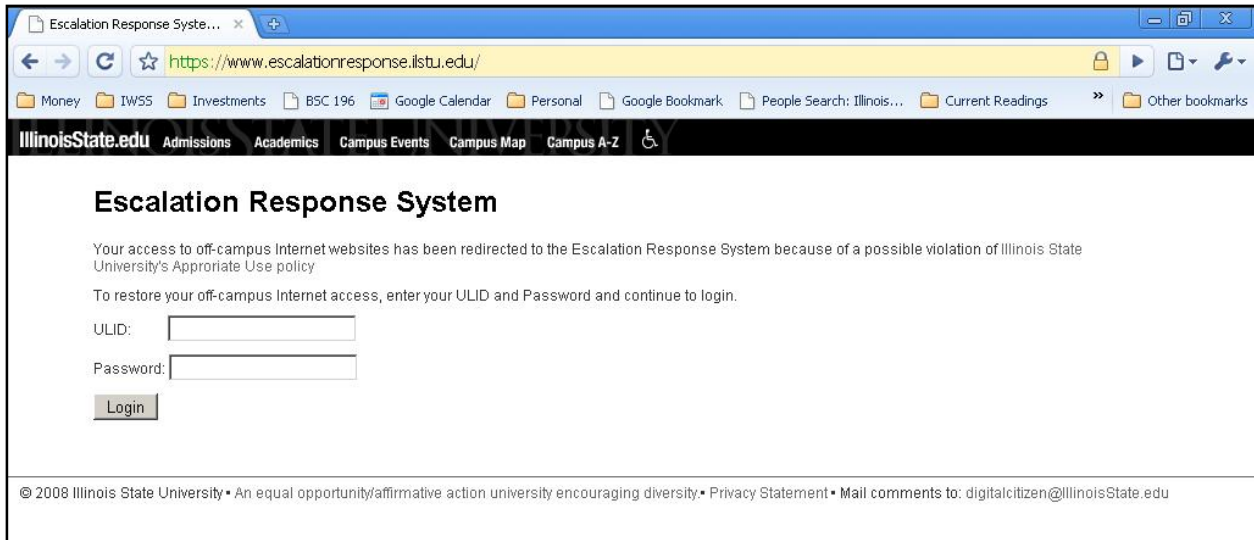
To avoid the Escalation Response system and associated penalties, do not engage in copyright infringement. Make sure you are not downloading or sharing music, movies, TV shows, etc. Consider removing P2P software from your computer; refer to <http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1380>.

For more information on the Escalation Response system, refer to the Digital Citizen Escalation System FAQ at <http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1379>.

Thank you,

Digital Citizen Project
Illinois State University
<http://www.digitalcitizen.ilstu.edu>

Appendix A4 First Level Violation Screens upon redirect



Appendix A4 (continued)
First Level Violation Screens upon redirect

The screenshot shows a web browser window with the address bar displaying <https://www.escalationresponse.ilstu.edu/escalation/level1/nextsteps.aspx>. The browser's bookmark bar includes items like Money, IW55, Investments, BSC 196, Google Calendar, Personal, Google Bookmark, People Search: Illinois..., Current Readings, and Other bookmarks. The navigation bar features the Illinois State University logo and links for Admissions, Academics, Campus Events, Campus Map, and Campus A-Z.

Escalation Response Level 1 Acknowledgement

Blocked Internet Access

Your off-campus Internet access will be blocked for 30 minutes. During this time, you can still access on-campus websites and resources. While Internet access in your room is blocked, you can still access the Internet in the following locations:

- University Computer Labs
- iSpot Ethernet Ports
- Campus Wireless

What Happens Next

Future attempts to download music illegally will lead to escalating penalties. If you continue to engage in copyright infringement, you will reach Escalation Level Two. Doing so will require you to complete an ethical exercise and will put you one step closer to disciplinary review by the Community Rights & Responsibilities (CR&R) office.

You can avoid future penalties. Do not download music illegally. Make sure all P2P software on your computer is turned off—even better, completely remove all P2P software from your computer. Step-by-step removal instructions.

Check out BirdTrax for a description of many of the legal alternatives mentioned below. BirdTrax is an Illinois State website that gives you the opportunity to learn about downloading legal music, movies, and TV.

Getting Help

Help is available at the following locations: University Computer Help Desk
Julian Hall 115
309-438-HELP(4357)

TechZone Walkup Center
Bone Student Center, Second Floor
309-438-7047

Community Rights & Responsibilities
Student Services Building 120
309-438-8621

Level 1 Escalation: Digital C... x

https://www.escalationresponse.ilstu.edu/escalation/level1/

Money IW55 Investments B5C 196 Google Calendar Personal Google Bookmark People Search: Illinois... Current Readings Other bookmarks

IllinoisState.edu Admissions Academics Campus Events Campus Map Campus A-Z

Escalation Level 1

Step 1: What is copyright?

According to the U.S. Copyright Office, copyright is a protection provided to "authors of [original works], including literary, dramatic, musical, artistic, and certain other intellectual works."

If a work is copyrighted, there are several restrictions on what you can do with it, unless you are the copyright holder. The owner of copyrighted material has exclusive rights to the work. The copyright holder can also give others permission to use the work in various ways.

For example, the music recordings made by Elvis Presley are owned by Sony BMG (RCA Records). As the copyright holder, Sony BMG has exclusive rights to say who can and cannot reproduce, distribute, and profit from musical recordings made by Elvis Presley.

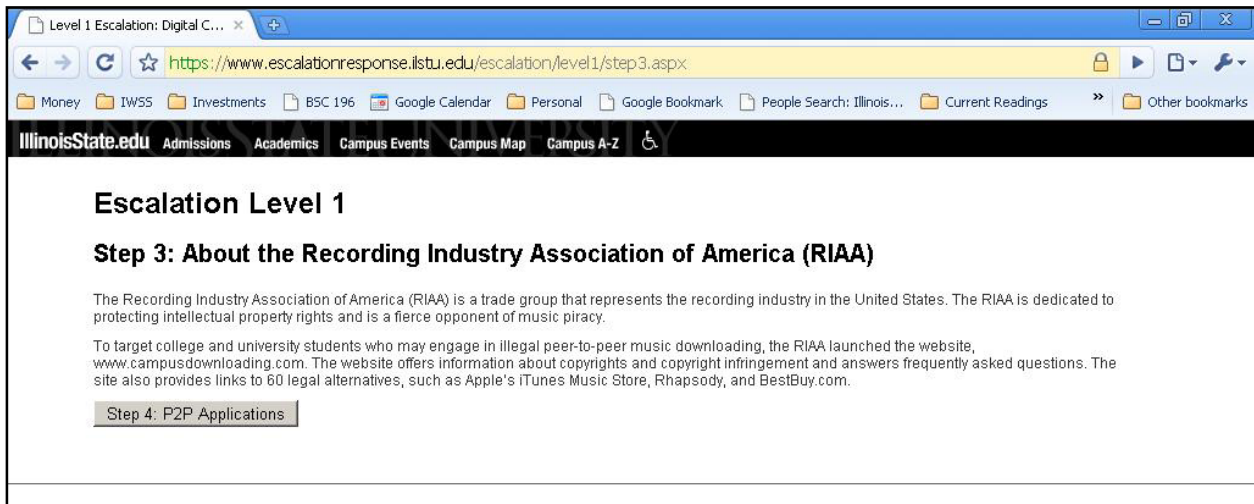
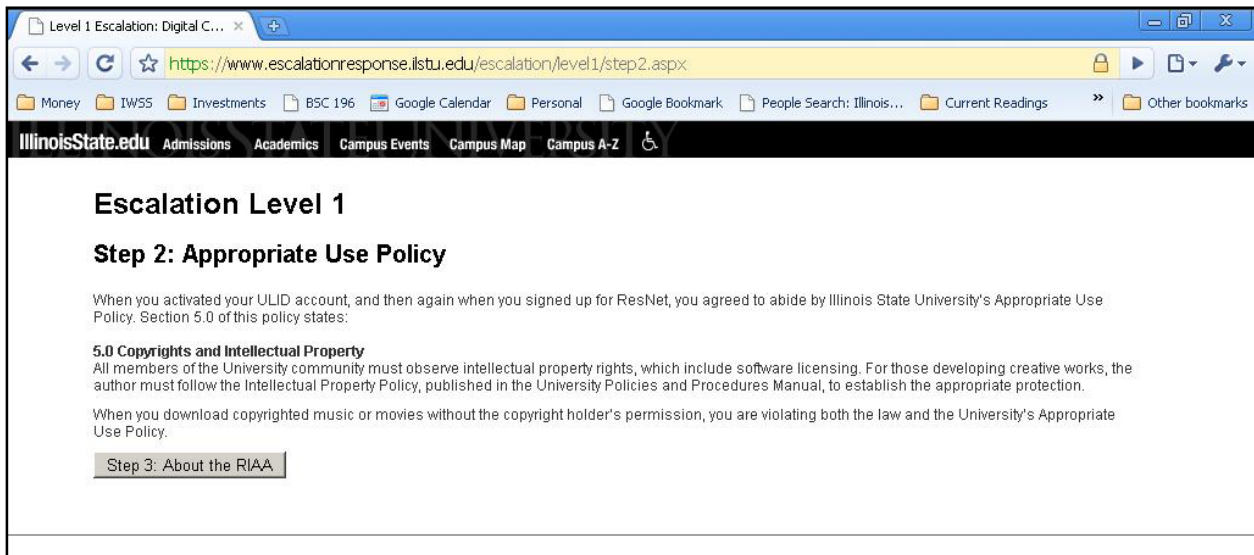
Unless you have permission, only the person (or entity) that holds the copyright can do the following:

- Reproduce the work (i.e. you cannot make copies of music or movies, except when you copy music and movies you already own for your personal use)
- Distribute the work (i.e. you cannot give copies of music or movies to others)

Actually, there are lots of other restrictions on copyrighted works, but the action items listed above are especially pertinent to music and movies. When you break the law by violating copyright, it is called "copyright infringement."

[Step 2: Appropriate Use Policy](#)

Appendix A4 (continued)
First Level Violation Screens upon redirect



Appendix A4 (continued) First Level Violation Screens upon redirect

The screenshot shows a web browser window with the URL <https://www.escalationresponse.ilstu.edu/escalation/level1/step4.aspx>. The page title is "Escalation Level 1" and the main heading is "Step 4: Peer-to-Peer (P2P) Applications Are Risky". The content discusses the risks of P2P file sharing applications like BearShare and LimeWire, including spyware and viruses. It provides instructions on how to remove P2P applications from a Windows or Mac computer. At the bottom of the page, there is a button labeled "Step 5: Legal Downloads".

Escalation Level 1

Step 4: Peer-to-Peer (P2P) Applications Are Risky

Peer-to-peer (P2P) file sharing applications like BearShare and LimeWire may put your computer at risk.

When you install a P2P file sharing application in Windows, it may carry spyware onto your computer. Spyware runs without your knowledge and monitors your Internet activities. Spyware can also create annoying pop-up advertisements and is often responsible for poor computer performance.

The files you download may also be unsafe. Viruses are sometimes disguised as songs or movies. When you download and try to play them, the virus infects your computer (instead of playing the song or movie you thought you were getting). It's always good practice to keep your anti-virus software up to date, but if you refrain from downloading files with P2P software, you can eliminate that risk altogether.

Unless you use P2P file sharing programs to download files legally, you should consider removing the software from your computer. If you use Windows, you can remove P2P applications through the Control Panel. If you have a Mac, you can remove P2P applications by deleting the program from the Application folder on your hard drive.

[Step 5: Legal Downloads](#)

The screenshot shows a web browser window with the URL <https://www.escalationresponse.ilstu.edu/escalation/level1/step5.aspx>. The page title is "Escalation Level 1" and the main heading is "Step 5: Legal Downloads". The content discusses legal alternatives to illegal downloading, including purchasing music CDs and movie DVDs, using online music services like iTunes, and using subscription models like Napster and Vongo.com. It also mentions free music sites like Pandora.com and Last.fm. At the bottom of the page, there is a button labeled "Step 6: Acknowledgement".

Escalation Level 1

Step 5: Legal Downloads

Aside from purchasing music CDs and movie DVDs, there are many legal alternatives to illegal downloading.

Many online music services allow you to download and pay for individual songs or albums. Among the most popular is iTunes, a service offered by Apple. Most online music vendors allow you to purchase individual songs for between \$.79 and \$.99 per song (or between \$8.99 and \$9.99 per album).

Some services even allow you to pay for and download movies. Using iTunes, you can buy movies and TV episodes and play them on your iPod or computer. Another online service, CinemaNow.com, allows you to download rented and purchased movies. You can burn the movies you buy to DVD (some movies are only watchable on your computer). If you're a Windows user, Amazon Unbox lets you rent or buy movies, which are downloaded to your computer. Downloadable movies generally sell for between \$9.99 and \$19.99 and TV show episodes can usually be purchased for \$1.99 each.

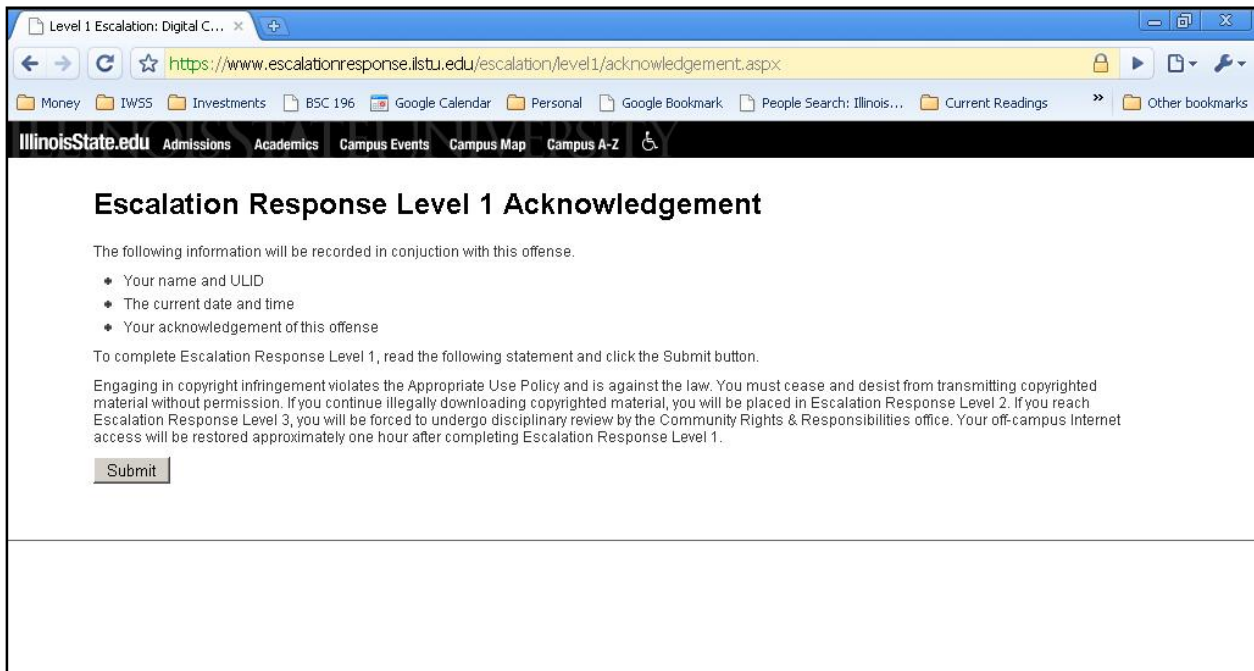
Instead of paying for each song or album individually, some companies operate using a subscription model. By paying a monthly fee, you gain access to a vast library of songs or movies. For example, Napster reportedly offers its subscribers unlimited access to five million songs. Vongo.com is an online movie service that offers its subscribers access to a library of movies viewable on demand. Subscription services like these typically charge around \$9.99 per month.

There are also a lot of free music sites that allow you to listen to popular songs on your computer. Pandora.com and Last.fm allow you to discover new music by playing artists you ask for, as well as songs the site thinks you might like. Shoutcast.com and Live365.com are two sites with a huge list of free, traditional radio stations.

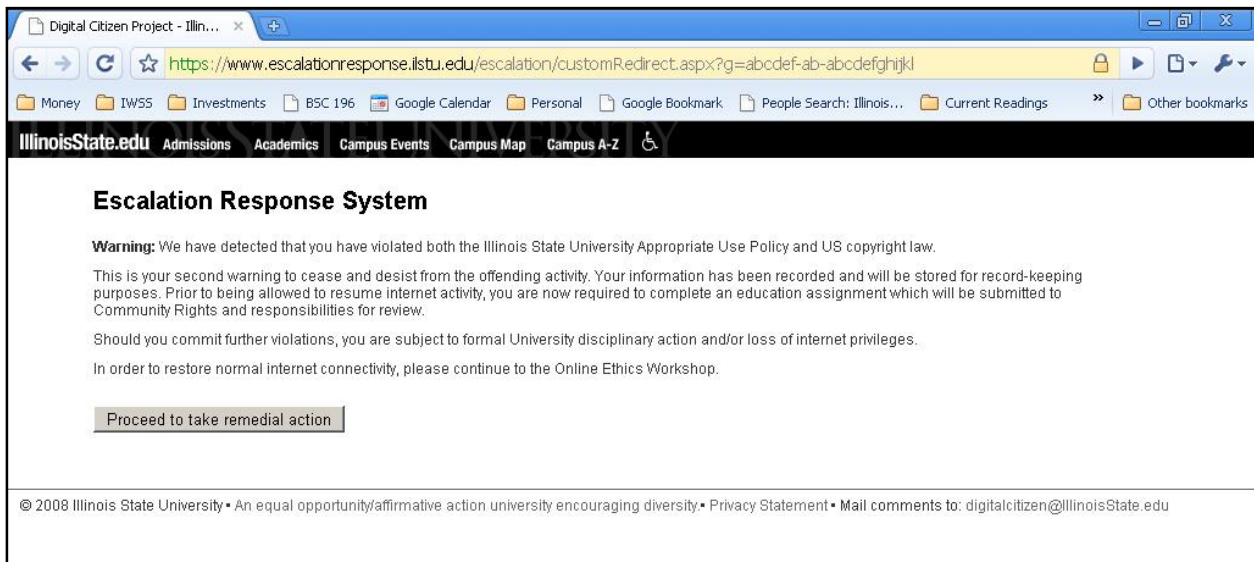
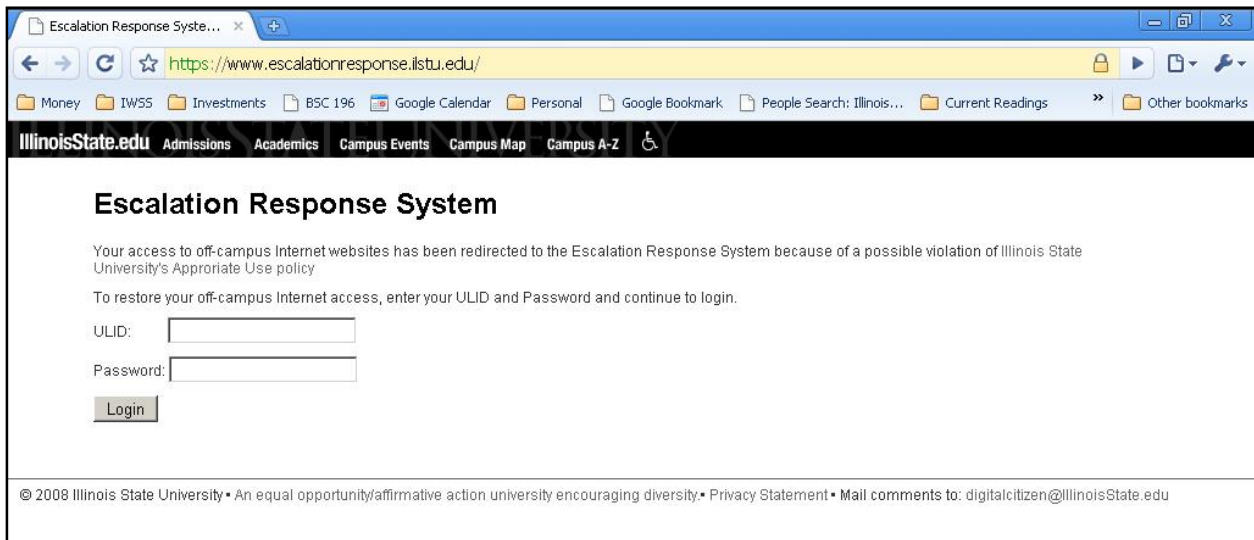
The number of legal alternatives to music and movie piracy is growing every day. You should explore these alternatives and find a solution that works for you.

[Step 6: Acknowledgement](#)

Appendix A4 (continued)
First Level Violation Screens upon redirect



Appendix A5 Second Level Violation Screens upon redirect



Appendix A5 (continued)
Second Level Violation Screens upon redirect

Level 1 Escalation: Digital C... x

https://www.escalationresponseilstu.edu/escalation/level2/nextsteps.aspx

Money IW55 Investments BSC 196 Google Calendar Personal Google Bookmark People Search: Illinois... Current Readings Other bookmarks

IllinoisState.edu Admissions Academics Campus Events Campus Map Campus A-Z

Escalation Response Level 1 Acknowledgement

Blocked Internet Access

This is your second offense. Your off-campus Internet access will be blocked for upto 4hours. During this time, you can still access on-campus websites and resources.
While Internet access in your room is blocked, you can still access the Internet in the following locations:

- University Computer Labs
- iSpot Ethernet Ports
- Campus Wireless

What Happens Next

Future attempts to download music illegally will result in severe disciplinary action taken against you.

If you continue to engage in copyright infringement, you will reach Escalation Level Three. Doing so will result in disciplinary review by the Community Rights & Responsibilities (CR&R) office. If you are found guilty by the Community Rights & Responsibilities office, you will lose your Internet access for the remainder of the semester.

You can avoid future disciplinary action. Do not download music illegally. Make sure all P2P software on your computer is turned off—strongly consider removing all P2P software from your computer. Step-by-step removal instructions.

Getting Help

Help is available at the following locations: University Computer Help Desk
Julian Hall 115
309-438-HELP(4357)

TechZone Walkup Center
Bone Student Center, Second Floor
309-438-7047

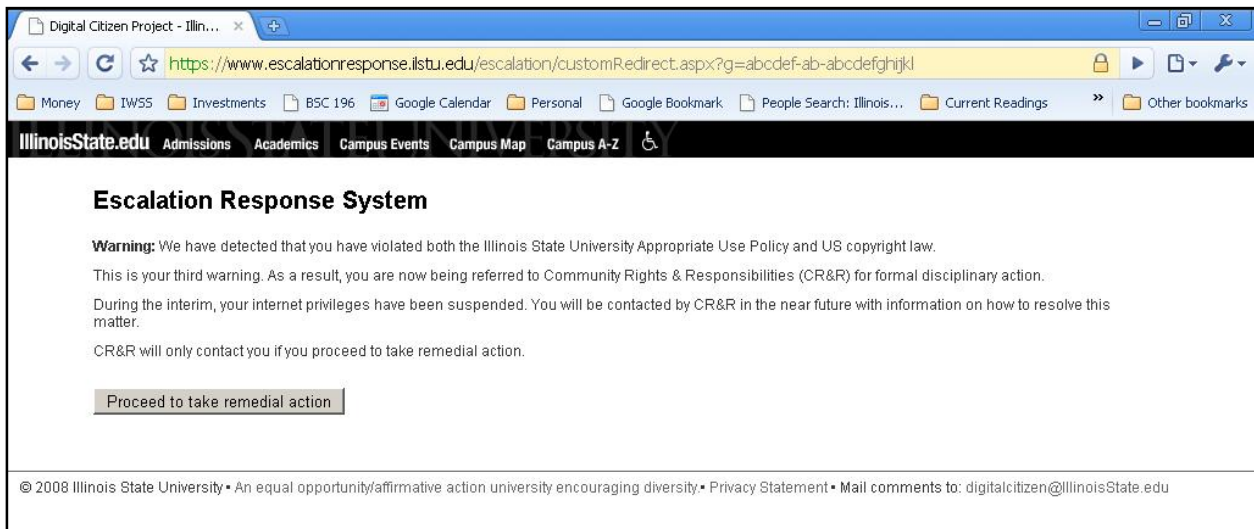
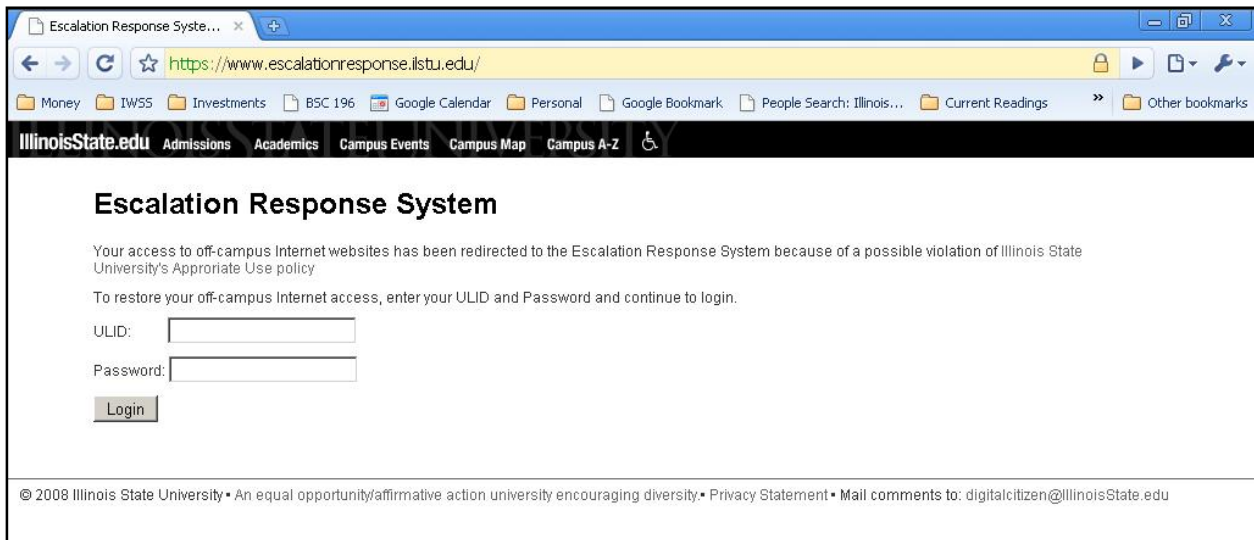
Community Rights & Responsibilities
Student Services Building 120
309-438-8621

Appendix A5 (continued)
Second Level Violation Screens upon redirect

The screenshot shows a web browser window with the following elements:

- Browser Tab:** Level 2 Escalation: Digital C...
- Address Bar:** <https://www.escalationresponse.ilstu.edu/escalation/level2/>
- Bookmarks Bar:** Money, IW55, Investments, BSC 196, Google Calendar, Personal, Google Bookmark, People Search: Illinois..., Current Readings, Other bookmarks
- Navigation Bar:** IllinoisState.edu, Admissions, Academics, Campus Events, Campus Map, Campus A-Z
- Page Content:**
 - Section Header:** Escalation Level 2
 - Sub-Header:** On-Line Ethics Workshop
 - Text:** The purpose of this assignment is to stimulate your thinking about the effects of an individual's actions upon others. This is intended to be a reflective assignment, and your completed work will not be evaluated on its content (other than to make sure you have answered all of the questions). You should utilize appropriate language, grammar, and spelling. You must complete all questions.
 - Text:** Please answer the following questions:
 - Question 1:** Reflect on the action which led to this sanction. Why do you think you are being asked to complete this workshop?
 - Question 2:** The University takes illegal file sharing seriously. How do you think the University and the University community are impacted by illegal on-line file sharing?
 - Question 3:** Reflect again upon the situation that led to you being assigned this workshop. Based on what you know, do you think your choices were ethical? Why or why not? If faced with a similar situation in the future, would you do anything differently? If so, what? If not, why not?
 - Button:** Submit your answers

Appendix A6 Third Level Violation Screens upon redirect



Appendix A6 (continued)
Third Level Violation Screens upon redirect

Level 3 Escalation: Digital C... x

https://www.escalationresponse.ilstu.edu/escalation/level3/Default.aspx

Money IW55 Investments B5C 196 Google Calendar Personal Google Bookmark People Search: Illinois... Current Readings Other bookmarks

IllinoisState.edu Admissions Academics Campus Events Campus Map Campus A-Z

Escalation Level 3

Blocked Internet Access

This is your third offense. Your off-campus Internet access will be blocked for the remainder of the semester. During this time, you can still access on-campus websites and resources.
While Internet access in your room is blocked, you can still access the Internet in the following locations:

- University Computer Labs
- iSpot Ethernet Ports
- Campus Wireless

Disciplinary Review

Due to your repeated copyright infringement, you have reached the final stage, Escalation Level Three. The Community Rights & Responsibilities office will contact you with more information.

Getting Help

Help is available at the following locations: University Computer Help Desk
Julian Hall 115
309-438-HELP(4357)

TechZone Walkup Center
Bone Student Center, Second Floor
309-438-7047

Community Rights & Responsibilities
Student Services Building 120
309-438-8621