

**Computing Studies**  
**College of Technology and Innovation**

**CST482/598**

**Network Forensics**

**Spring 2012**

**SYLLABUS**

Instructor: Bruce R. Millard  
Office Peralta 230A  
Phone: 727-1734  
Office Hours: see my Web site

Teaching Assistant: none

Lecture: 9:00 – 10:15 PM Monday & Wednesday in Peralta 201

Schedule Line Number: 12586/12579

Description:

Use and creation of advanced network forensics tools: intrusion detection and prevention, honeynets, traffic routing and management, and data reduction and graphing tools.

Prerequisite: CST 481, programming experience and CST 489 expected

Overrides: No capacity overrides will be given. The instructor may give prerequisite overrides to qualified students.

Required Text:

*Building Open Source Network Security Tools: Components and Techniques,*  
Mike Shiffman, 2001, Wiley, ISBN 0471205443

*Network Security Tools,*

N. Dhanjani and J. Clarke, April 2005, Oreilly Media, ISBN 0596007949

<u>Grading:</u>	Projects	45	
	Midterm exam	25	
	Class participation	5	
	Final Exam	<u>25</u>	Comprehensive
		100	

See the class web page or page 3 of the syllabus on grading appeals and cheating for information on those topics.

Course Grade: based on points (absolute, fixed, no curve)

<u>CST 482</u>		<u>CST 598</u>	
>= 96.0	A+	>= 98.0	A+
>= 90.0 < 96.0	A	>= 92.0 < 98.0	A
>= 88.0 < 90.0	A-	>= 90.0 < 92.0	A-
>= 85.0 < 88.0	B+	>= 87.5 < 90.0	B+
>= 80.5 < 85.0	B	>= 82.5 < 87.5	B
>= 78.0 < 80.5	B-	>= 80.0 < 82.5	B-
>= 75.0 < 78.0	C+	>= 77.5 < 80.0	C+
>= 70.0 < 75.0	C	>= 70.0 < 77.5	C
>= 60.0 < 70.0	D	>= 60.0 < 70.0	D
< 60.0	E	< 60.0	E

**Computing Studies**  
College of Technology and Innovation

**CST482/598**

**Network Forensics**

**Spring 2012**

## Tentative Schedule

<b>Week</b>	<b>Date</b>	<b>Topics</b>	<b>Assignment</b>	<b>Reading*</b>
<b>1</b>	Jan 9	Introduction	P0.5	
<b>2</b>	Jan 11, 18	Data Man. (pgp) & Incidents	P0.5 due, P1	N3
<b>3</b>	Jan 23, 25	Tools (install & use)	P1 due	N1
<b>4</b>	Jan 30, Feb 1	Tools (use & extensions)	P2	N2
<b>5</b>	Feb 6, 8	Tools (use & extensions)	P3	N4, N5, N6
<b>6</b>	Feb 13, 15	Tools (system & network logs)	P2 due	Everything so far
<b>7</b>	Feb 20, 22	<b>Midterm Exam Review</b>	P3 due	Everything so far
<b>8</b>	Feb 27, 29	<b>Midterm Exam</b>	P4 avail	N11
<b>9</b>	Mar 5, 7	Tools (programming extensions)	P5 avail	1, 2, 3
	Mar 19 - 25	<b>Spring Break</b>	P4 due	
<b>10</b>	Mar 26, 28	Tools (programming extensions)		8, 10
<b>11</b>	Apr 2, 4	Network programming libraries	P5 due	
<b>12</b>	Apr 9, 11	Creating a new tool	P6 avail	
<b>13</b>	Apr 16, 18	Creating a new tool		
<b>14</b>	Apr 26, 28	Creating a new tool		
<b>15</b>	Apr 24	<b>Final Review</b>	P6 due	Everything
	TBD	<b>Final Exam</b>		(Comprehensive)

**To get a broader idea of the course see**

<http://dcs.asu.edu/faculty/BruceMillard/CST482/CST%20482%20Description.doc>

\* Numbers are Chapter and Appendix numbers from the 1st required textbook. The Nxx, reading is from the 2<sup>nd</sup> required text (Network Security Tools). Reading includes any additional class handouts that may appear because of limitations in the text and information necessary for programming projects.

**Dates of note:**

<b>Drop/Add deadline</b>	<b>Jan 11</b>
<b>MLK day</b>	<b>Jan 16</b>
<b>Spring Break</b>	<b>Mar 19 – 25</b>
<b>Course Withdrawal Deadline</b>	<b>Mar 28</b>
<b>Last day of class</b>	<b>Apr 24</b>
<b>Complete Withdrawal Deadline</b>	<b>Apr 24</b>
<b>Reading day</b>	<b>Apr 25</b>
<b>Final Exam</b>	<b>TBD</b>
<b>Last day of Final Exams</b>	<b>May 2</b>

**No late assignments (homework or project) will be accepted without prior approval from the instructor. No make-up exams will be given without written documentation of illness or prior approval from instructor.**

## **Supplementary Information**

### **ADA Statement**

The Americans with Disabilities Act (ADA) is a federal antidiscrimination statute that provides comprehensive civil rights protection for persons with disabilities. One element of this legislation requires that all qualified students with documented disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation please contact the Disability Resource Center at ASU Polytechnic located in Student Affairs Quad # 4 or call 480-727-1039 / TTY: 480-727-1009. Eligibility and documentation policies online: <http://www.asu.edu/studentaffairs/ed/drc/>

### **Class Cheating Policy**

While discussions between students are encouraged, cheating in this course will not be tolerated. Any student found cheating on an exam or assignment may be given a failing grade for the course and flagrant violations can result in additional consequences. You are cheating if you represent someone else's work as your own or if someone else represents your work as his or hers. All graded work (exams, programming assignments, as well as any written exercises or quizzes) in this class must represent your own individual work only. Students may discuss the conceptual aspects of an assignment, but in solving programming and other assignments, students must turn in their own, independently developed solutions. Grading may include executing software on your solutions that compares the structure and content of your solution files with that of other students. Any case of suspected cheating will be referred directly to the College of Technology and Applied Sciences according to established policy. By your registration in this class, you are assumed to have read, understand and agreed to this policy, as well as to the procedures conveyed at the web sites below.

- Studentlife's Student Academic Integrity Policy  
[http://www.asu.edu/studentaffairs/studentlife/judicial/academic\\_integrity.htm](http://www.asu.edu/studentaffairs/studentlife/judicial/academic_integrity.htm)
- ASU's policy on Academic Dishonesty in the Student Code of Conduct:  
<http://www.asu.edu/aad/manuals/usi/usi104-01.html>
- DCS's Academic Integrity Information Page:  
<http://www.east.asu.edu/ctas/dcst/Students/cheating.html>

One ramification of this policy is that every student must assure that neither an electronic nor hard copy of their work gets into the hands of another student. You must know how to use access control to protect your files and you may not share a computing system that does not have access control with another student in this class, without taking special steps to ensure privacy of your files. If someone else in the class steals your homework (with or without your knowledge,) then you may both get failing marks for the course.

### **Class Grading Appeals Policy**

Each class assessment/learning tool (i.e., test, quiz, homework or programming assignment) is assigned a relative grade. This grade is converted, using a tool specific multiplier) to form part of the student's overall grade for the class. Occasionally, inadvertent miss grading or misinterpretations of either the tool or grading response may occur. On such occasions, the student must immediately bring the issue to the instructor's attention. In the case of material returned to the student in class the questioned item(s) must be addressed at that time (at the end of the class period) or left with the instructor for later review with the student. Materials submitted electronically will result in an assessment handed out in class or via e-mail on a case-by-case and class-by-class basis. Appeals for results-only assessments may be handled electronically.