ITMS 483 RUBRIC

ITMS 483 Digital Evidence
Students may be scored on a scale of 1 to 5; scores of 2 and 4 may be interpolated.

Program Educational Objectives			
Objective **Score ▶**	**5**	**3**	**1**
Investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law	The student is consistently able to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law	The student is generally able to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of laws	The student is unable to investigate information security incidents and violation of law using computer resources in a manner such that all evidence is usable for fault analysis and, when applicable, admissible in a court of law
Course student outcomes Upon completion of this course the student should be able to do the following:			
Outcome **Score ▶**	**5**	**3**	**1**
Acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner	The student is consistently able to acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner	The student is often able to acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner	The student is unable to acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner
Recall and describe law, theories, techniques, and practices that apply to digital forensic investigations	The student is able to recall and describe law, theories, techniques, and practices that apply to digital forensic investigations accurately and in detail	The student is able to recall and describe law, theories, techniques, and practices that apply to digital forensic investigations with some omissions or inaccuracies	The student is unable to recall and describe law, theories, techniques, and practices that apply to digital forensic investigations
Identify and describe types of computer and Internet crimes	The student is able to identify and describe types of computer and Internet crimes accurately and in detail	The student is able to identify and describe types of computer and Internet crimes with some omissions or inaccuracies	The student is unable to identify and describe types of computer and Internet crimes
Preserve and process a crime scene involving digital evidence	The student is fully able to preserve and process a crime scene involving digital evidence	The student is somewhat able to preserve and process a crime scene involving digital evidence	The student is unable to preserve and process a crime scene involving digital evidence
Explain the legal procedures and standards in the collection and analysis of digital evidence	The student is able to explain the legal procedures and standards in the collection and analysis of digital evidence accurately and in detail	The student is able to explain the legal procedures and standards in the collection and analysis of digital evidence with some omissions or inaccuracies	The student is unable to explain the legal procedures and standards in the collection and analysis of digital evidence
Prepare a report of a digital investigation for appropriate stakeholders and defend your findings	The student has clearly demonstrated their ability to prepare a report of a digital investigation for appropriate stakeholders and defend their findings	The student has demonstrated to some extent their ability to prepare a report of a digital investigation for appropriate stakeholders and defend their findings	The student is unable to prepare a report of a digital investigation for appropriate stakeholders and defend their findings
Present an analysis of digital evidence in a legal or ad-ministrative proceeding as an expert witness	The student has clearly demonstrated their ability to present an analysis of digital evidence in a legal or administrative proceeding as an expert witness	The student has demonstrated to some extent their ability to present an analysis of digital evidence in a legal or administrative proceeding as an expert witness	The student is unable to present an analysis of digital evidence in a legal or administrative proceeding as an expert witness
Apply security principles and practices to maintain operations in the presence of risks and threats	The student has clearly demonstrated their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student has demonstrated to some extent their ability to apply security principles and practices to maintain operations in the presence of risks and threats	The student is unable to demonstrate an ability to apply security principles and practices to maintain operations in the presence of risks and threats