### SY386: Cyber Crime Investigations

### Assigned: 3th Week of classes

You have been placed in teams of 4. Each team will choose a project from below.

# Project A: Scenario

The goal is to imagine and emulate a cybercrime scenario in a controlled environment, resulting in the creation of digital artifacts that can be forensically analyzed.

An example from Digital Corpora:

# Your final product should resemble something like this:

# The expected deliverable for this project will look similar to what on this page:

<http://forensicscontest.com/puzzles>

Other places to look for crime summary:

<http://digitalcorpora.org/corpora/scenarios/>

<http://www.cfreds.nist.gov/dfrws/>

<http://dftt.sourceforge.net/>

# Project B: Tool development

# The goal is to design and implement a forensic tool or a module to an existing tool. Example tools that have been developed for projects can be found here:

1. Here are examples of tools implemented for some digital forensic competition.

<http://forensicscontest.com/puzzles>

<http://forensicscontest.com/tools>

1. List of digital forensic tools from Wikipedia

<https://en.wikipedia.org/wiki/List_of_digital_forensics_tools>

1. Kali toolkit tools

<http://tools.kali.org/tools-listing>

# Project C: Research Study (a maximum of 40 pages for the write-up)

The goal is to perform a study of a relevant subject in the context of digital forensics.

1. Because of the international character of many cybercrimes, criminal investigations now require international legal frameworks. Sometimes investigations have to be stopped if it is not clear whether the IT infrastructure where the evidence is located.

The research study will address questions like: How are countries dealing with the investigation of international cybercrime? How is collection of international evidence taking place? Are there explicit investigative powers? What US laws apply? The development of cloud services and the fact the often ISPs are located in either one or a small number of countries, whilst their users are located in many more countries makes international is making it even more complex.

1. Technological developments that are currently still in their Infancy will have an impact on security, investigations and law enforcement in the near future. For example, the further digitization of motor vehicles and household products (internet of things) and the dark web will impact the way investigations are carried out. Society and law enforcement must prepare for this. Research questions in this context are: how are these recent developments affecting security and investigations processes? What consequences does this have for law enforcement? How can parties involved in the fight against cybercrime prepare for this? How are these investigations being handled?

# Project 4: Your choice

Come up with own relevant project has to be approved by Dr. Shumba.

# Grading of Projects:

1. Project Proposal (10%) – due February 8th (place in your Team folder)
2. Project checkpoint (20%) – due March 22th – In-class presentation
3. Final Project submission and public defense (55%) April 22nd – 26th
4. Peer evaluation - 15%