



COURSE: Computer Forensics & Investigation

MARKS:

CODE: BCN3193

ASSESSMENT: Quiz 1

DURATION:

Evidence Collection

xCriminal is accused in a digital crime of customers information theft in xCity bank. The theft crime has been launched in the period between 12:15:38:34 and 12:25:38:34 on 19th February, 2015. After preliminary investigations procedures, investigators discovered that xCriminal hide some digital evidences as an ambient data in his laptop. Consequently, the investigators have preserved xCriminal's Laptop and immediately started investigating its storage media. Unfortunately, the investigator found that the laptop's disk was correctly partitioned and it was in "shut down" mode. As a computer forensic investigator, analyze this case and show how the hidden digital evidences can be extracted from xCriminal Labtop.

- (a) Assume the digital evidence extraced in (b) is a part of deleted file which include metadata as shown in the table below.

U_ID	Log_in_time	Log_out_time	Event	Transaction
xCriminal	12:09:38:34	12:29:15:20	Accessing bank server database	SQL injection in accounts table

Analyze the obtained evidence and evalute if it is convincing to juries, and in conformity with common law and legislative rules.

End of Quiz 1