Reg. No.

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

III SEMESTER MCA END SEMESTER EXAMINATIONS,

DEC 2020-JAN 2021

SUBJECT: CYBER FORENSICS [MCA 5030]

REVISED CREDIT SYSTEM

Time: 3 Hours 04/01/2021 MAX.: 50 MARKS

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A.	Explain the Internet Security Hierarchy with help of a neat diagram.	**05**
1B.	Explain the importance of "competitive intelligence" based deterrence approach in foreseeing or mitigating cyber forensic scenario.	**03**
1C.	Describe the prime objectives and priorities in cyber forensics.	**02**
2A.	Explain the secure payment solutions with its security features and standard compliances.	**05**
2B.	Explain the methodologies to address business issues: Trust, Control, and Accountability in an Identity Management System.	**03**
2C.	Discuss the difference between IDS and IPS.	**02**
3A.	Explain the data backup systems and its role in data recovery.	**05**
3B.	Describe sessioning in computer networks and discuss its importance in a network forensic scenario.	**03**
3C.	A Middletown man charged with allegedly setting fire to his home in 2016 is back in custody and awaiting trial. Ross Compton, 60, was indicted in January for aggravated arson and insurance fraud for allegedly setting fire to his Court Donegal house. The blaze caused nearly $400,000 in damages.	**02**

Compton, who had been free on his own recognizance, failed to show up for a court hearing in March, just days before his trial in Butler County Common Pleas Court, and Judge Charles Pater issued a warrant for his arrest.

On Tuesday, Compton appeared before Pater and said he was confused about the date for his last hearing. Pater set bond at $100,000, and Compton is scheduled to be back in court on Aug. 14.

Compton was arrested after the fire based in part from data taken from his pacemaker.

The case is believed to be the first of its kind to use data from a beating heart as evidence. Last year, Pater ruled that evidence from Compton's pacemaker could be presented at trial.

Middletown detectives said Compton gave statements that were "inconsistent" with evidence collected at the scene and from his medical device.

Compton, who has an artificial heart implant that uses an external pump, told police he was asleep when the fire started. When he awoke and saw the fire, he told police he packed some belongings in a suitcase and bags, broke out the glass of his bedroom window with a cane, and threw the bags and suitcase out the window before climbing out the window himself and taking the bags to his car.

Police then obtained a search warrant for all of the electronic data stored in Compton's cardiac pacing device, according to court records.

The data taken from Compton's pacemaker included his heart rate, pacer demand, and cardiac rhythms before, during and after the fire.

A cardiologist who reviewed that data determined "it is highly improbable Mr. Compton would have been able to collect, pack and remove the number of items from the house, exit his bedroom window and carry numerous large and heavy items to the front of his residence during the short period of time he has indicated due to his medical conditions," according to court documents.

Compton's former defense attorney Glenn Rossi argued the pacemaker evidence should be thrown out because the search was an invasion of Compton's constitutional rights and unreasonable seizure of his private information.

*Note: A **pacemaker** is a small device that's placed in the chest or abdomen to help control abnormal heart rhythms.*

Review the above case as a cyber-forensics expert, and explain the roles and responsibilities.

4A.	In a cyber-forensics scenario, pulling system from the network or keeping it offline seems to tricking decision for an expert. Explain the awareness features cyber expert need to exhibit, with help of a real time case.	**05**
4B.	Discuss the outline of email retention policy that the service providers need to adhere to. Describe its reflections, when it comes to email forensics?	**03**
4C.	How do you interpret the following two scenarios, as cyber-forensics personnel? **Scenario One** An IT manager reviews a detection tool report that indicates a company employee is accessing restricted Internet sites and downloading objectionable material. After discovering the activity, the IT manager remotely accesses the employee's personal computer to obtain evidence. The employee is then dismissed, based on the evidence located and obtained. **Scenario Two** An IT manager reviews a detection tool report indicating a company employee is accessing restricted Internet sites and downloading objectionable material. After discovering this activity, the IT manager follows procedures, reporting his suspicions to the nominated computer incident response contact, in this case the chief information officer(CIO). The CIO then invokes the company's incident response plan by contacting the incident response team, which includes computer forensics experts. This team isolates the offending machine; conducts a forensic examination of the computer system following methodologies known to be acceptable to criminal, civil, and arbitration courts or tribunals; and establishes where the material came from, how often, and who else knew about it. By following its effective policies and procedures, the organization (via the CIO) is in an excellent position to take immediate legal and decisive action based on all the available facts and evidence.	**02**
5A.	Explain mobile device tool classification system with help of a diagram.	**05**
5B.	Explain the NIST guidelines to Enterprise Risk Officers and risk committees for translating cybersecurity to ERM.	**03**
5C.	When forensic work is complete, regenerate the message digest values using the backups on which work was performed; log these new values alongside the hashes that were originally generated. If the new values match the originals, it's reasonable to	**02**

	conclude that no evidence tampering took place during the forensic examination of the information file(s). Discuss is the significance of this activity?	