BINUS UNIVERSITY INTERNATIONAL

COMP6348001
Network Forensics

SCU	3 Credit(s)	
Contact Hours	3 x 50 minute-lectures per week	
Pre-requisite(s)	Computer Networks and Security	
Teaching Team	Kalpin Erlangga S, S.Si., M.Kom	kalpin@gmail.com

Course Outline
Odd Semester 2021-2022

Syllabus Prepared by	Raymond Bahana, ST., M.Sc & Kalpin Erlangga S, S.Si., M.Kom

Reviewed by	Diah Wihardini, B.Sc.(Hons)., M.Ed., Ph.D.
Checked by	Raymond Bahana, ST., M.Sc Raymondus Raymond Kosala, Ph.D
Approved by	Raymondus Raymond Kosala, Ph.D.
Updated on	02/08/2018

BINUS UNIVERSITY INTERNATIONAL
The Joseph Wibowo Center for Advanced Learning (JWC)
JL. Hang Lekir I No. 6, Senayan, Jakarta 10270, Indonesia

Version	:	2	Revision Date	:	-
Revision	:	0	Effective From	:	September 17, 2018

1. Course Description

The course is designed to understand network forensics through case study and laboratory exercises. It shows the educational benefit from understanding methodology and procedures of digital forensics in network to find any issues such as malware, hacking, and performance against the network. Students need to understand about application, protocols, topologies, routing, and devices which required to perform forensic analysis in the network. Students will learn about law and ethical in network forensics, controlling digital evidence as a part of digital forensics process, network forensics principles and documentation of network forensics. This course will combine study case and laboratory exercises beside of theoretical which given in the class with expectation output as research paper related to the network forensics.

2. Study Program Specific Outcomes

Study Program Specific Outcomes	
SO – 3	Able to assess technology trend in informatics area to deliver alternative solution of software development;
SO – 6	Able to communicate and utilize the latest trend in technology to contribute in the global workforce.

3. Learning Outcomes

Upon successful completion of this course, students are expected to be able to:

1. Identify different techniques of capturing digital evidence from a scene in network forensics, technology, and principles
2. Define appropriate tools necessary to sample, seal, and dissect a given intrusion evidence, and concept of network forensics and traffic analysis
3. Conduct laboratory experiments in network forensics and evidence handling
4. Analyze a case file or correlation log to find the root cause and warrant corrective action
5. Evaluate the impact of the incident to the victim organization, network traffic analysis and intrusion detection from wired and wireless networks

4. Course Structure

Throughout the semester, there are 3 x 50-minute lectures and hands-on exercises per week for this course. The lecturer facilitates learning by giving lectures on the theories and providing exercise problems to be discussed during the weekly tutorials. As this is a demanding course, the course requires full commitment and motivation to do an independent study outside classroom. Students are expected to write their own lecture notes and actively work on the given problems in order to optimize their learning in the classroom. Furthermore, for summative assessment purposes, a mid-semester examination is conducted to assess the student’s understanding of the first-half of the topics, while the rest of the topics are examined in the final examination at the end of semester.

5. Course Requirements

Each student is required to have his/her own laptop.
Students must have knowledge in basic networking and information technology fundamentals.

6. Text and Other Resources

6.1. Text

- Davidoff, S., & Ham, J. (2012). *Network forensics: tracking hackers through cyberspace*. Prentice Hall. ISBN: 978-0-13-256471-7

6.2. Other Resources

- Luttgens, J. , & Pepe, M., (2014). *Incident response & computer forensics* (3rd Ed.). McGraw-Hill. ISBN: 978-0071798686
- Datt, S., (2016). *Learning network forensics*. Packt Publishing. ISBN: 978-1-78217-490-5
- Nelson, B. and Phillips, A. (2015). *Guide to computer forensics and investigation*S (5th Ed.). Cengage Learning. ISBN: 978-1285060033

7. Schedule

Week	Topics	References	Learning Outcomes
1.	Network Forensics Introduction	Network Forensics Chapter 1.1-1.5	LO 1
2.	Sources of Evidence	Network Forensics Chapter 2.1 Incident Response & Computer Forensics Chapter 9	LO 1, LO 2
3.	Understanding TCP/IP Protocols	Network Forensics Chapter 2.2	LO 1, LO 2
4.	Evidence Acquisition	Network Forensics Chapter 3.1-3.3	LO 1, LO 2, LO 3
5.	Traffic Analysis	Network Forensics Chapter 4.1-4.4	LO 1, LO 2, LO 4
6.	Statistical Flow Analysis	Network Forensics Chapter 5.1-5.7	LO 1, LO 2, LO 4
7.	Network Forensics Wireless	Network Forensics Chapter 6.1-6.5 Learning Network Forensics Chapter 4	LO 1, LO 2, LO 3
8.	Tracking Intruders on the Network Understanding Network Intrusion Detection/Prevention Systems	Network Forensics Chapter 7.1-7.9 Learning Network Forensics Chapter 5	LO 2, LO 3, LO 4, LO 5
9.	Event Log Correlation and Analysis	Network Forensics Chapter 8 Learning Network Forensics Chapter 6	LO 2, LO 4
10.	Switches, Routers, and Firewalls	Network Forensics Chapter 9 Learning Network Forensics Chapter 7	LO 1, LO 2, LO 3
11.	Web Proxies and Tunneling	Network Forensics Chapter 10.1-10.6, 11.1-11.3	LO 1, LO 2, LO 3
12.	Malware in Network Forensics	Network Forensics Chapter 12	LO 2, LO 4, LO 5
13.	Final Project Presentation / Guest Lecture		LO 1, 2, 3, 4

8. Assessment

8.1. Assessment Summary

The assessment for the defined course learning outcomes will be conducted throughout the course as detailed in Section 8.4. The assessment summary and alignment between the assessment tasks and the course objectives is defined in the table below. A list of assessment rubrics used will also be provided, indicating the assessment standards and criteria that a student can follow to succeed in this course.

No.	Components	Percentage	Learning Outcomes
1.	Quiz	10 %	LO 1, LO 3, LO 5
2.	Project	50 %	LO 1, LO 2, LO 3, LO 4
3.	Mid-Examination	20 %	LO 1, LO 2
4.	Final Examination	20 %	LO 1, LO 2, LO 5
	Total	100 %	

8.2. Class Policies

To optimize individual learning, students are expected to:

- Attend all lectures since failure to attend a set number of lectures may prohibit the student to sit in the examinations (as indicated in the Student Handbook);
- Read the textbook on the prescribed topics and the tutorial questions prior to the scheduled lectures and tutorials;
- Proactively review their own learning progress and approach the lecturer/tutor as soon as an additional academic assistance is needed;
- Periodically access their New Binus Maya account to download lecture notes, if provided; and
- Work individually on each quiz, some of which may be given without any previous notice.

8.3. Submission and Collection of Assessment

In regard to the given assignments, students are expected to:

- Periodically access their New Binus Maya account to download the tutorial assignment questions;
- Submit the assignment by the given due date since a late submission will not be accepted;
- Work individually on either home written and computing assignments although performing a group-study is encouraged.

8.4 Assessment Descriptions

1. Assessment Task 1: Quiz

   Five to ten-minutes quizzes are given throughout the semester, of which the top four are summed up for the final grade of this part.

2. Assessment Task 2: Project

   The semester project consist of 2 parts: research project (60%) and research paper (40%). Students will form a project team and propose a research project (their own research project or available topics provided by the lecturer). Once approved, each of the team performs their own project and evaluate their results based on the proposed methodology and measurement. The team then write a research paper based on the research project they have done. The research paper has a minimum of 5 pages with **IEEE-style template**. The structure of the research paper should be as follows:

   I. Introduction
   Show the background and motivation of why the research is important.

   II. Related Works
   Cite what are similar other works.

   III. Design of the System
   Describe the architecture of the proposed system.

   IV. Results
   Show a graph or table of the measured results.

   V. Discussion
   Discuss the significance of the findings.

   VI. References
   Use the IEEE-style referencing.

   The research paper, which is written in a .doc, .docx, or .pdf file, is to be handed in electronically by the end of the semester. If the research paper successful published by local or international publisher then the student will get full score for project.

3. Assessment Task 3: Mid-Examination
Individual Mid-examination is written in the form of short answers, essay, and/or problem solving that students will have to answer during the scheduled exam time. The exact schedule of exam time will be advised later.

4. Assessment Task 4: Final Examination
Individual Final examination is written in the form of short answers, essay, and/or problem solving that students will have to answer during the scheduled exam time. The exact schedule of exam time will be advised later.

9. General Information

Students are required to be familiar with the BINUS UNIVERSITY - Code of Conduct, and to abide by its terms and conditions.

9.1 Copying of Copyright Material by Student

A condition of acceptance as a student is the obligation to abide by the University's policy on the copying of copyright material. This obligation covers photocopying of any material using the University's photocopying machines, and the recording off air, and making subsequent copies, of radio or television broadcasts, and photocopying textbooks. Students who flagrantly disregard University policy and copyright requirements will be liable to disciplinary action under the Code of Conduct.

9.2 Academic Misconduct

Please refer to the Code of Conduct for definitions and penalties for Academic Misconduct, plagiarism, collusion, and other specific acts of academic dishonesty.

Academic honesty is crucial to a student's credibility and self-esteem, and ultimately reflects the values and morals of the University as a whole. A student may work together with one or a group of students discussing assignment content, identifying relevant references, and debating issues relevant to the subject. Academic investigation is not limited to the views and opinions of one individual, but is built by forming opinion based on past and present work in the field. It is legitimate and appropriate to synthesize the work of others, provided that such work is clearly and accurately referenced.

Plagiarism occurs when the work (including such things as text, figures, ideas, or conceptual structure, whether verbatim or not) created by another person or persons is used and presented as one's own creation, unless the source of each quotation or piece of borrowed material is acknowledged with an appropriate citation.

Encouraging or assisting another person to commit plagiarism is a form of improper collusion and may attract the same penalties.

To prevent Academic Misconduct occurring, students are expected to familiarize themselves with the University policy, the Subject Outline statements, and specific assignment guidelines. Students should also seek advice from Subject Leaders on acceptable academic conduct.

9.2.1 Guidelines to Avoid Plagiarism

Whenever you copy more than a few words from any source, you must acknowledge that source by putting the quote in quotation marks and providing the name of the author. Full details must be provided in your bibliography.

If you copy a diagram, statistical table, map, etc., you must acknowledge the source. The recommended way is to show this under the diagram. If you quote any statistics in your text, the source should be acknowledged. Again full details must be provided in your bibliography.

Whenever you use the ideas of any other author you should acknowledge those, using the APA (American Psychological Association) style of referencing.

Students are encouraged to co-operate, but collusion is a form of cheating. Students may use any sources (acknowledged of course) other than the assignments of fellow students. Unless your Subject Leader informs you otherwise, the following guideline should be used:

Students may work together in obtaining references, discussing the content of the references and discussing the assignment, but when they write, they must write alone.

9.2.2 Referencing for Written Work (where applicable)

Referencing is necessary to acknowledge others' ideas, avoid plagiarism, and allow readers to access those others' ideas. Referencing should:

1. Acknowledge others' ideas;
2. Allow readers to find the source;
3. Be consistent in format and
4. Acknowledge the source of the referencing format.

To attain these qualities, the school recommends use of either the Harvard or American Psychological Association (APA) style of referencing, both of which use the author/date.

9.2.3 Referencing Standards

APA style referencing.

9.2.4. Disclaimer

Every effort will be made to ensure that the teaching, learning and assessment activities of this course are given as described. Any unpublished changes for course improvement will be notified and discussed in class. However, circumstances may occasionally make this impossible, and BINUS UNIVERSITY therefore reserves the right to add, alter or withdraw particular information contained in this course outline.

Version	:	2	Revision Date	:	-
Revision	:	0	Effective From	:	September 17, 2018

Approval

Prepared by,	**Reviewed by,**
Kalpin Erlangga S, S.Si., M.Kom, BINUS UNIVERSITY INTERNATIONAL	**Diah Wihardini, B.Sc.(Hons)., M.Ed., Ph.D.** Manager of Learning and Faculty Development BINUS UNIVERSITY INTERNATIONAL
Checked by,	**Checked by,**
Raymond Bahana, ST., M.Sc Subject Content Coordinator - Computer Science Program BINUS UNIVERSITY INTERNATIONAL	**Raymond Kosala, Ph.D.** Head of Program - Computer Science BINUS UNIVERSITY INTERNATIONAL

Approved by,
Raymond Kosala, Ph.D. Dean, Faculty of Commuting and Media BINUS UNIVERSITY INTERNATIONAL

APPENDIX-1: ASSESSMENT RUBRICS

Assessment Task 2: Project

Learning Outcomes	**Assessment Indicators**	**Proficiency Level**				
		Poor (D – 1)	**Average (C – 2)**	**Good (B – 3)**	**Excellent (A – 4)**	**Mark**
1. Identify different techniques of capturing digital evidence from a scene		*Not demonstrated, limited description of the techniques*	*Adequate description of techniques*	*Good and detailed outline, clear and justifiable techniques and their relevance to the advantages/disadvantages*	*Detailed outline, in-depth justification of the techniques, high relevance to the captured fingerprint*	
	1.1. Background					
	1.2. Variety of techniques					
	1.3. (Dis)advantages					
2. Define appropriate tools necessary to sample, seal, and dissect a given intrusion evidence, and concept of network forensics and traffic analysis		*Not demonstrated, Limited understanding about tools to be use.*	*Adequate understanding about tools to be use.*	*Good and can use tools of network forensics and traffic analysis with expected output.*	*Excellent in using tools of network forensics and traffic analysis with expected output.*	
	xxx					
3. Conduct laboratory experiments in network forensics and evidence handling		*Not demonstrated, Could not identify problems and no output*	*Adequate, can identify problem in network through forensics. Demonstrate evidence handling*	*Good in identifying problem in network and report with correct way in evidence handling*	*Excellent identifying problem in network and provide comprehensive report. Excellent in evidence handling.*	
	3.1 Challenges					
	3.2 Output					
4. Analyze a case file or correlation log to find the root cause and warrant corrective action		*Not demonstrated, methods & analysis hardly addressing the problem*	*Adequate, methods & analysis are related to the problem to an extent*	*Correct methodology and analysis*	*Thorough and highly relevant yet concise methodology and analysis*	
	4.1. Framework					
	4.2. Evaluation					
Total Marks						

APPENDIX-2: TEACHING, LEARNING AND ASSESSMENT PLAN (only for Lecturer's own discretion)

Week	Topic	Learning Outcome	Time	Learning Activity	Resource needed	Formative Assessment	Summative Assessment
1	Network Forensics Introduction	Summarize the entire course and prepare the required software	50 min	Lecture presentation	Lecture slides	-	Mid-Exam
		Identify the components of network environment and its functions	50 min	Lecture presentation			
		Describe the methodology of Network Forensics Investigation (OSCAR)	50 min	Lecture presentation			
2	Sources of Evidence	Identify sources of evidence in network	50 min	Lecture presentation Exercise	Lecture slides Problems to solve	Exercise	
		Exercises read data from sources of evidence in network	100 min	Hands-on experiments			
3	Understanding TCP/IP Protocols	Describe TCP/IP Protocols and its features	100 min	Lecture presentation Exercise	Lecture slides Wireshark	Exercise	
		Exercises: using wireshark to read data in network		Hands-on experiments			
4	Evidence Acquisition	Describe terms of passive and active evidence	50 min	Lecture presentation Quiz	Lecture slides Problems to solve	Quiz	

		acquisition Hands-on experiments to receive network data, services, and logging	100 min	Hands-on experiments			
5	Traffic Analysis	Capturing traffic in network devices Conduct traffic analysis: protocol analysis, packet analysis, reconstruct higher-layer protocol data from streams	50 min 100 min	Lecture presentation Exercises Lecture presentation Hands-on experiments	Lecture slides Problems to solve	Exercise	
6	Statistical Flow Analysis	Identify compromised hosts according to statistical flow analysis Summary flow records information through components: sensor, collector, aggregator, analysis with experiments	50 min 100 min	Lecture presentation Exercise Lecture presentation Hands-on experiments	Lecture slides Problems to solve	Exercise	
7	Network Forensics Wireless	Identify rogue wireless access points Investigate malicious activity that occurred using wireless network. Investigate attacks against wireless network through experiment	50 min 100 min	Lecture presentation Exercise Hands-on experiments	Lecture slides Problems to solve	Exercise & Presentation	
8	Tracking Intruders on the Network	Understand ways and means of intrusion and prevention	50 min	Lecture presentation	Lecture slides Problems to solve	Exercise	Final Exam

	Understanding Network Intrusion Detection/Prevention Systems	Detect and track intruders in the network Configuring NIDS/NIPS to detect events which may not define before.	100 min	Hands-on experiments Lecture presentation Exercise			
9	Event Log Correlation and Analysis	Extract information from event logs Identify sources of network event logs Describe methods of collection and aggregation architectures of log	50 min 50 min 50 min	Lecture presentation Exercise Lecture presentation Hands-on experiments	Lecture slides Problems to solve	Exercise	
10	Switches, Routers, and Firewalls	Understand the features and configuration of switches, routers, and firewalls Finding evidence from storage media of switches, routers, and firewalls Analyze evidence from storage media of switches, routers, and firewalls	50 min 100 min	Lecture presentation Exercise	Lecture slides Problems to solve	Quiz	
11	Web Proxies and Tunneling	Identify and detect proxying (web) and network tunnel through various protocols	150 min	Case study	Problems to solve	Exercise	
12	Malware in	Understanding malware	50 min	Lecture presentation	Lecture slides	Quiz	

	Network Forensics	and its different types Identify and detect malware attack Tracking down the source of malware and containing an infection	 50 min 50 min	Exercise Lecture presentation Exercise	Problems to solve		
13	Final Project Presentation / Guest Lecture	Present research paper related to course topic.	150 min	Student presentation	Presentation materials	Presentation	