**MANCHESTER METROPOLITAN UNIVERSITY**

**School of Computing, Mathematics & Digital Technology**

**ASSIGNMENT COVER SHEET**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Unit: | 6G6Z1013 |
| Assignment set by: | Dr. Robert Hegarty (Part 1) and Dr. Liangxiu Han (Part 2) |
| Verified by: | Dr. Liangxiu Han (Part 1) and Dr. Robert Hegarty (Part 2) |
| Moderated by: | Thomas Martin |
| Assignment number: | 1CWK50 |
| Assignment title: | Network and Internet Forensics |
| Type: (GROUP/INDIVIDUAL) | Individual Report |
| Hand-in format and mechanism: | via Unit area on Moodle |
| Deadline: | As indicated on Moodle. |

Learning Outcomes Assessed:

1. Conduct synthetic analysis of a digital forensic investigation from the initial response through to completion of an investigation for example, what types of evidence (e.g., network traffic, etc.) can be collected, why are they important to a forensic investigation and how may evidence be analysed and interpreted?
2. Critically evaluate recent developments in Computing Forensics.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

It is your responsibility to ensure that your work is complete and available for assessment by the date given on Moodle. If submitting via Moodle, you are advised to check your work after upload; and that all content is accessible. Do not alter after the deadline. You should make at least one full backup copy of your work.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Penalties for late hand-in: see Regulations for Undergraduate Programmes of Study: <http://www.mmu.ac.uk/academic/casqe/regulations/assessment.php>. The timeliness of submissions is strictly monitored and enforced.

Exceptional Factors affecting your performance: see Regulations for Undergraduate Programmes of Study : <http://www.mmu.ac.uk/academic/casqe/regulations/assessment/docs/ug-regs.pdf>

Plagiarism: Plagiarism is the unacknowledged representation of another person’s work, or use of their ideas, as one’s own. MMU takes care to detect plagiarism, employs plagiarism detection software, and imposes severe penalties, as outlined in the Student Handbook (<http://www.mmu.ac.uk/academic/casqe/regulations/docs/policies_regulations.pdf> and Regulations for Undergraduate Programmes (<http://www.mmu.ac.uk/academic/casqe/regulations/assessment.php> ). Bad referencing or submitting the wrong assignment may still be treated as plagiarism. If in doubt, seek advice from your tutor.

|  |  |
| --- | --- |
| Assessment Criteria: | Indicated in the attached assignment specification. |
| Formative Feedback: | Formative feedback (individual oral feedback) for Part 1A and Part 1B will be provided in class on 31st October and 12th , December respectively. For Part 2, the formative feedback (individual oral feedback) will be provided during the lab sessions and staff contact hours. Two check points : 1. Week commence of 23-01 – check point 1 for the topic;  2. Week commence of 13/03 – check point 2 for the informal feedbacks on the report content. |
| Summative Feedback format: | Detail comments will be provided within individual reports |
| Weighting: | This Assignment is weighted at 50% of the total unit assessment. |

**FACULTY OF SCIENCE AND ENGINEERING**

**SCHOOL OF**

**COURSEWORK TEMPLATE 2016/17**

|  |  |  |  |
| --- | --- | --- | --- |
| **UNIT CODE:**  6G6Z1013 | | **UNIT TITLE:**  Network and Internet Forensics | |
| **ASSESSMENT ID:**  1 | **ASSESSMENT DESCRIPTION**:  Report | | **WEIGHTING:**  50% |
| * 1. **The aim of this assignment**   This assignment aims to measure the unit specific learning outcomes of Network and Internet Forensics Specifically, through this assignment, students will learn to:   1. Conduct synthetic analysis of a digital forensic investigation from the initial response through to completion of an investigation for example, what types of evidence (e.g., network traffic, etc.) can be collected, why are they important to a forensic investigation and how may evidence be analysed and interpreted? 2. Critically evaluate recent developments in Computing Forensics   **The coursework is therefore divided into two parts: Part 1 aims to measure the firs learning outcome and the Part 2 aims to measure the second learning outcome.**  **Staff contact hours available on the unit Moodle area for providing help and support.** Part 1 – A – Capture Analysis Carry out and document analysis of each of the 3 network captures (trace files) provided, using Wireshark. Create a narrative for the events occurring in each of the network captures, identify and describe any malicious activity detected in the captures. Your report should be around 1000 words (This is just a guideline. There is no penalty on word count. Less or more than 1000 should be fine as long as your report clearly and concisely addresses all the specifications).  The structure for the report on each capture should follow the format below:   1. Capture number, your name, your student number 2. Capture Overview - A list of the computers taking part in the capture. Provide a name, description and IP address for each computer. (Be consistent when referring to computers by name throughout the report) 3. Malicious Behaviour - Describe any evidence of malicious behaviour that you find in the network captures. Some behaviour may appear to be benign, yet have a malicious intent. 4. Mitigation of malicious behaviour - Describe the steps that you may take to mitigate the effects of any malicious activities you detect in the captures. These steps may be technical, or policy based. 5. Reference – Provide references for any of the sources that you cite in your report.   Note: Regarding Formatting   * Font 11, Times New Roman. * Use a cover page with the title, your name and student ID on it. * Provide a table of contents and your abstract on separate pages, at the start of the document * Use the Harvard referencing system to cite others work (Tip; Install and use reference management software such as Mendeley).   **Formative feedback for Part 1A will be provided in class on 31st October, you will receive individual oral feedback on your work.** Part 1 – B – Coding & Documentation Write a Python script that parses a capture file and visualises the results. Your script should satisfy the following requirements:   1. Take a capture file and IP address as arguments at the command line e.g.    1. PortGraph.py Capture1.pcap 192.168.1.1 2. Graph the destination port of the packets against the time stamp of the packets. 3. Graph only TCP traffic from the specified IP address. 4. Display appropriate X & Y axis labels on the graph. 5. Display your student number as the graph title.   Use your code to create a graph from Capture1.pcap. Describe the trend shown in the graph produced by your code, include a figure showing your graph. Explain how your script can be used to identify attacks. Your report should be around 1,000 words.  Note: Include your source code in the appendix of your report.  **Formative feedback for Part 1B will be provided in class on 12th December, you will receive individual oral feedback on your work.** Part 2 Write a report about a recent development in Network and Internet Forensics. (around 1000 - 2,000 words excluding the references and abstract. This is just a guideline. There is no penalty on word count. Less or more than 2000 should be fine as long as your report clearly and concisely addresses all the specifications). You may select your own topic, or choose one from the reading list provided. The report should focus on the state of the art on identification, collection or analysis of evidence (e.g. the sources of evidences can be from computer hardware, file systems, network devices, network protocols). Some example topics could be: research into network-based evidence at the transport layer, analysis of memory content, analysis of network traffic, etc. Note that your chosen topic should be different from your final year project.  The report, for the chosen topic should cover a) What are the existing methods? b) How each of the current existing methods works? c) What’s the difference between each method used (comparison study), critical analysis and evaluation of your topic. The report is not simply to be a cut-and-paste from some the literature. All reports will be checked with a plagiarism checker. Any works not references will be assumed to be your own.    Please note the report should include and be structured in the following way:   1. Title, and your name with your student ID ( This should be on a cover page) 2. A table of contents 3. Abstract 4. Introduction 5. Literature review study, comparison and critical analysis and evaluation 6. Conclusion 7. References (Citations)   Note: More information on report formatting:   * Font 11, Times New Roman. * Use a cover page with the title, your name and student ID on it. * Provide a table of contents and your abstract on separate pages * Use the Harvard referencing system to cite others work (Tip; Install and use reference management software such as Mendeley).   **Formative feedback for Part 2 will be provided in lab sessions and contact hours, you will receive individual oral feedback on your work.** The timeline for this assignment You should submit your report through Moodle by the deadlines below. Late submission will not be accepted. Extensions can only be granted via exceptional factors and PLPs if negotiable deadlines etc. are stated.   |  |  | | --- | --- | | **Action for each student** | **Deadline** | | Assignment submission | Friday, 24th March, 2017 |   **Appendix: The Reading List of some useful research papers ( your topics are not necessary from this list. You may find some other papers you are interested from the internet).**  **Research Papers:**   * **Surveys**   1. “Security, privacy and trust in Internet of Things: The road ahead”, S.Sicari, A. Rizzardi, et al, Computer Networks, vol.76, 2014, pp. 146-167   2. “The Internet of Things vision: Key features, applications and open issues”, Eleonora Borgia, Computer Communications, 2014, pp.1–31   3. “Internet of Things – New security and privacy challenges” Rolf H. Weber, Computer Law and security review, 2010, pp. 23–30,   4. "[A Survey on Internet Traffic Identification](http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5208732&userType=inst)," Callado, Carlos Kamienski, Geza Szabo, Balazs Gero, Judith Kelner, Stenio Fernandes, Djamel Sadok, IEEE Communications Surveys & Tutorials, Vol. 11, No. 3. (2009), pp. 37-52.   5. "[A Survey of Techniques for Internet Traffic Classification Using Machine Learning](http://caia.swin.edu.au/cv/garmitage/things/Nguyen_Armitage_SurveysAndTutorials2008.pdf)," T. Naguyen and G. Armitage, IEEE Communications Surveys and Tutorials, 2008   6. "[A Taxonomy of DDoS attacks and DDoS defense Mechanisms](http://portal.acm.org/citation.cfm?id=997156)," Jelena Mirkovic and Peter Reiher. ACM Computer Communication Review, Volume 34 Issue 2, April 2004, pp. 39-53.   7. "[Anomaly detection: A survey](http://portal.acm.org/citation.cfm?id=1541882)," V. Chandola, A. Banerjee and V. Kumar, ACM Computing Surveys, Vol. 41, Issue 3, July 2009, pp. 15:1-15:58. * **Cloud Forensics**   1. **“**Legal Process and Requirements for Cloud Forensic Investigations**”,** I. Orton, A. Alva, et al. - Cybercrime and Cloud Forensics: Applications for Investigation Processes 2013, pp.186-229   2. **“Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics”, G. Grispos, T. Storer, and W. Glisson, International Journal of Digital Crime and Forensics, 4(2), 2012, pp.28-48.**   3. **“**Seizing Electronic Evidence from Cloud Computing Environments**”,** Josiah Dykstra, Cybercrime and Cloud Forensics: Applications for Investigation Processes ,2013   4. **“**Cloud forensics: An overview**”,** Keyun Ruan, Joe Carthy, Tahar Kechadi, Mark Crosbie, <http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf>   5. **Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing,** Richmond Journal of Law and Technology 19,2012, [http://www.cs.umbc.edu/~dykstra/Final-Dykstra-Riehl-1.pdf](http://www.cs.umbc.edu/%7Edykstra/Final-Dykstra-Riehl-1.pdf)   **Other related papers can be found here**  **http://www.forensicswiki.org/wiki/Cloud\_Forensics\_Bibliography**   * **Network Security**   1. \*["Snort Lightweight Intrusion Detection for Networks,"](http://www.usenix.org/event/lisa99/full_papers/roesch/roesch.pdf) M. Roesch, Proceedings of LISA '99: 13th Systems Administration Conference Seattle, Washington, USA, November 1999, pp. 229-238.   2. \*"[Diagnosing network-wide traffic anomalies](http://portal.acm.org/citation.cfm?id=1015492)," A. Lakhina, M. Crovella, and C. Diot, ACM SIGCOMM 20004, pp. 219-230.   3. \*"[A Taxonomy of DDoS attacks and DDoS defense Mechanisms](http://portal.acm.org/citation.cfm?id=997156)," Jelena Mirkovic and Peter Reiher. ACM Computer Communication Review, Volume 34 Issue 2, April 2004, pp. 39-53.   4. \*"[Botnet Detection Based on Network Behavior](http://www.springerlink.com/content/n77m076734522777/)", W. Strayer, David Lapsely, Robert Walsh and Carl Livadas, Advances in Information Security, 2008, Volume 36, 1-24.   5. "[DDoS attack detection method using cluster analysis](http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V03-4N206XS-2&_user=30343&_coverDate=04%2F30%2F2008&_alid=1729548594&_rdoc=1&_fmt=high&_orig=search&_origin=search&_zone=rslt_list_item&_cdi=5635&_sort=r&_st=13&_docanchor=&view=c&_ct=120&_acct=C000003998&_version=1&_urlVersion=0&_userid=30343&md5=8ff3af153a87eac49eef9a2e1726431a&searchtype=a)," K. Lee, J. Kim, K. Kwon, Y. Han and S. Kim, Expert Systems with Applications, Volume 34, Issue 3, April 2008, Pages 1659-1665.   6. \*[Modeling and Automated Containment of Worms](http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4358715)," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, Vol. 5, No. 2, APRIL-JUNE 2008, pp. 71-86.   7. \*[BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection](http://www.usenix.org/events/sec08/tech/full_papers/gu/gu.pdf)," G. Gu, R. Perdisci, J. Zhang and W. Lee, 17th USENIX Security Symposium, 2008, pp. 139-154.   8. \*"[Anomaly-based network intrusion detection: Techniques, systems and challenges](http://ceres.ugr.es/%7Egmacia/papers/COMSEC09_AnidsPublishedVersion.pdf)", P. Garcia-Tedodro, J. Diaz-Verdejo, G.Macia-Fernandez and E. Vazquez, Computers & Security, Vol. 28, 2009, pp. 18-28.   9. "[Anomaly detection: A survey](http://portal.acm.org/citation.cfm?id=1541882)," V. Chandola, A. Banerjee and V. Kumar, ACM Computing Surveys, Vol. 41, Issue 3, July 2009, pp. 15:1-15:58.   10. "[BotGrep: Finding P2P Bots with Structured Graph Analysis](http://www.usenix.org/events/sec10/tech/full_papers/Nagaraja.pdf)," S. Nagaraja, P. Mittal, C. Hong, M. Caesar, and N. Borisov, USENIX Security 2010, Washington DC, USA, August 2010, pp. 1-16.   11. \*[Top 10 Computer Viruses and Worms](http://abcnews.go.com/Technology/top-computer-viruses-worms-internet-history/story?id=8480794), ABC News, Sept. 2009. * **Traffic Measurement and Analysis**   1. "Seven Years and One Day: Sketching the Evolution of Internet Traffic," P. Borgnat, G. Dewael, K. Fukuda, P. Abry, and K. Cho, IEEE INFOCOM 2009, Rio de Janeiro, Brazil, April, 2009, pp.711--719.   2. "On the stability of the information carried by traffic flow features at the packet level," A. Este, F. Gringoli, and L. Salgarelli. SIGCOMM Comput. Commun. Rev., 39(3):13.18, 2009.   3. "Unveiling core network-wide communication patterns through application traffic activity graph decomposition," Y. Jin, E. Sharafuddin, and Z.-L. Zhang, ACM SIGMETRICS, 2009.   4. "On Dominant Characteristics of Residential Broadband Internet Traffic," G. Maierm, A. Feldmann, V. Paxson and M. Allman, ACM SIGCOMM IMC, 2009   5. "Profiling the End Host," T. Karagiannis and K. Papagiannaki, N. Taft and M. Faloutsos, Pasive and Active Measurement, 2007   6. "Network Traffic Characteristics of Data Centers in the Wild," T. Benson, A. Akella and D. Maltz, ACM IMC, 2010.   7. "Characterizing the Global Impact of the P2P Overlay on the AS-level Underlay," A. Rasti, R. Rejaie and W. Willinger, Passive and Active Measurement, Zurich, Switzerland, Apr. 7-9, 2010.   8. "Youtube traffic characterization: a view from the edge," P. Gill, M. Arlitt, Z. Li and A. Mahanti, ACM IMC, 2007. * **Application Traffic Monitoring and Identification**   1. "Internet Traffic Classification Demystified: On the Sources of the Discriminative Power," Y. Lim, H. Kim, J. Jeong, C. Kim, T. Kwon, and Y. Choi, ACM SIGCOMM CoNEXT, Philadelphia, PA, Dec. 2010.   2. "Early application identification," L. Bernaille, R. Teixeira, and K. Salamatian, ACM CoNEXT, 2006.   3. "Traffic classification through simple statistical fingerprinting," M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli, SIGCOMM Comput. Commun. Rev., 37(1):5.16, 2007.   4. "Graph-based p2p traffic classification at the internet backbone," M. Iliofotou, H.-c. Kim, M. Faloutsos, M. Mitzenmacher, P. Pappu, and G. Varghese, IEEE INFOCOM, 2009.   5. "Comparing traffic classifiers," L. Salgarelli, F. Gringoli, and T. Karagiannis, SIGCOMM Comput. Commun. Rev., 37(3):65.68, 2007.   6. "BLINC: Multilevel Traffic Classification in the Dark," T. Karagiannis, K. Papagiannaki, and M. Faloutsos, ACM SIGCOMM, Philadelphia, PA, August 2005.   7. "PortLoad: taking the best of two worlds in traffic classification," Giuseppe Aceto, Alberto Dainotti, Walter de Donato, Antonio Pescape, IEEE INFOCOM, 2010   8. "Lightweight, payload-based traffic classification: An experimental evaluation," M. Morandi O. Baldini A. Monclus P. Risso, F. Baldi, ICC08, May 2008. * **Social Network & Mobile Traffic**   1. "An Analysis of Social Network-Based Sybil Defenses," Bimal Viswanath, Ansley Post, Krishna P. Gummadi, Alan Mislove, ACM SIGCOMM, 2010.   2. "You are who you know: Inferring user profiles in online social networks," A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel. In Proc. WSDM10, New York, NY, Feb 2010.   3. " User Interactions in Social Networks and their Implications," C. Wilson, B. Boe, A. Sala, K. P. N. Puttaswamy, and B. Y. Zhao. In Proc. Eurosys09, Nuremberg, Germany, Apr 2009.   4. "Comparison of Online Social Relations in Terms of Volume vs. Interaction: A Case Study of Cyworld", H. Chun, H. Kwak, Y. Eom, Y. Ahn, S. Moon, H. Jeong, ACM SIGCOMM IMC 200.   5. "Analysis of topological characteristics of huge online social networking services," Y.-Y. Ahn, WWW 07, New York, NY, USA, 2007.   6. "Statistical properties of community structure in large social and information networks," J. Leskovec, WWW08, New York, NY, USA, 2008.   7. "A First Look at Traffic on Smartphones, H. Falaki, D. Lymberopoulos, R. Mahajan, S. Kandula, and D. Estrin, ACM Internet Measurement Conference, Melbourne, Australia, Nov. 1-3, 2010.   8. "A First Look at Mobile Hand-held Device Traffic," G. Maier, F. Schneider, and A. Feldmann, Passive and Active Measurement, Zurich, Switzerland, Apr. 7-9, 2010.   9. "A Comparative Study of Handheld and Non-Handheld Traffic in Campus WiFi Networks," A. Gember, A. Anand, and A. Akella, Passive and Active Measurement, Atlanta, USA, Mar. 20-22, 2011.   10. "Measurement Analysis of Mobile Data Networks," Young J. Won, B.C. Park, S.C. Hong, K.B. Jung, H.T. Ju, and James W. Hong, Passive and Active Measurement Conference (PAM 2007), Louvain-la-neuve, Belgium, Apr. 5-6, 2007, pp. 223-227. * **Network Performance / Virtualization**   1. "Characterizing user behavior and network performance in a public wireless LAN," A. Balachandran, G. Voelker, P. Bahl, P. Rangan, ACM SIGMETRICS, 2002.   2. "Netgauge: A Network Performance Measurement Framework," T. Hoefler, T. Mehlan, A. Lumsdaine and W. Rehm, Proceedings of High Performance Computing and Communications (HPCC), Sep. 2007, pp.659--671.   3. "WiMAX Performance Evaluation," P. Mach, R. Bestak, Sixth International Conference on Networking (ICN'07), Apr. 22-28, 2007, pp.17--20.   4. "Mobile WiMAX systems: performance and evolution", F. Wang, A. Ghosh, C. Sankaran, P. Fleming, F. Hsieh, and S. Benes, IEEE Communications Magazine, Vol.46, Issue. 10, Oct. 2008, pp.41--49.   5. "Best-case WiBro performance for a single flow," S. Woo, K. Jang, S. Kim, S. Cho, J. Lee, Y. Lee, S. Moon, ACM Workshop on Mobile Internet through Cellular Networks: Operations, Challenges, and Solutions (MICNET), October 2009, Beijing, China.   6. "Evaluation of VoIP Quality over WiBro," M. Han, Y. Lee, S. Moon, K. Jang, D. Lee, Passive and Active Measurement Conference (PAM), April 2008.   7. "Performance Impact of Large File Transfer on Web Proxy Caching: A Case Study in a High Bandwidth Campus Network Environment," H. Kim, D. Lee, K. Chon, B. Jang, T. Kwon, and Y. Choi, Journal of Communications and Networks, Volume 12, Number 1, Feb. 2010. * **Social Networks Analysis**   1. Toes and Owda, Template-Based Information Extraction System for Detection of Events on Twitter, 2013 International Conference on Cybercrime, Security and Digital Forensics, Cardiff.   2. Appelt, D. E., 1999. Introduction to Information Extraction. Ai Communications, 12(3), pp. 161-172.   3. BBC, 2012. Huge rise in social media 'crimes'. [Online] Available at: http://www.bbc.co.uk/news/uk-20851797   4. Farber, D., 2012. Twitter hits 400 million tweets per day, mostly mobile. [Online]  Available at: http://news.cnet.com/8301-1023\_3-57448388-93/twitter-hits-400-million-tweets-per-day-mostly-mobile/ [Accessed 10 April 2013].   5. Friedland, G. & Sommer, R., 2010. Cybercasing the Joint: On the Privacy Implications of Geotagging. Washington, D.C., s.n.   6. Hannay, P. & Baatard, G., 2011. GeoIntelligence: Data Mining Locational Social Media Content for Profiling and Information Gathering. Perth, s.n.   7. Knott, E. & Owda, M., 2012. The detection of potentially illegal activity on financial discussion boards using information extraction. London, UK, s.n.   8. Lawrence, S., Giles, C. L. & Bollacker, K., 1999. Digital libraries and autonomous citation indexing. Computer, 32(6), pp. 67-71.   9. Li, R., Lei, K. H., Khadiwala, R. & Chang, K. C.-C., 2012. TEDAS: a Twitter Based Event Detection and Analysis System. Washington, DC, USA, IEEE, pp. 1273-1276.   10. Li, W., Eickhoff, C. & de Vries, A. P., 2012. Want a coffee?: predicting users' trails. Portland, Oregon, ACM, pp. 1171-1172.   11. Oussalah, M., Bhat, F., Challis, K. & C., S., 2011. A software architecture for Twitter collection, search and geolocation services. Knowledge-Based Systems, Volume 37, pp. 105-120.   12. Sankaranarayanan, J. et al., 2009. Twitterstand: news in tweets. Seattle, Washington, USA, ACM, pp. 42-51.   13. Watanabe, K., Ochi, M., Okabe, M. & Onai, R., 2011. Jasmine: A Real-time Local-event Detection System based on Geolocation Information Propagated to Microblogs. Glasgow, Scotland, ACM, pp. 2541-2544. | | | |
| **NAME OF STAFF SETTING ASSIGNMENT: Liangxiu Han and Robert Hegarty** | | | |
| **DOCUMENT UPDATED: 19/09/2016** | | | |