TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#0: Intro & Logictics
Spring 2023

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn

Thông tin môn học

- Tên môn: Pháp chứng kỹ thuật số (Digital forensics)
- Mã môn: NT334
- Khối kiến thức: Chuyên ngành
- Số tín chỉ: 03
  - Lý thuyết: 02
  - Thực hành: 01 (HT1)

Nội dung môn học

- **Mục tiêu:**

  Trang bị những kiến thức cơ bản về điều tra bằng chứng số, tội phạm số trên các thiết bị điện tử.

- **Nội dung:**
  - Các khái niệm tổng quan về khoa học điều tra số
  - Quy trình và yêu cầu điều tra
  - Điều tra số trên các môi trường khác nhau
  - Viết báo cáo, trình bày kết quả điều tra.

Nội dung môn học

- Các khái niệm cơ bản về pháp chứng
- Pháp chứng máy tính
- Pháp chứng bộ nhớ RAM
- Pháp chứng HĐH, bộ nhớ lưu trữ
- Pháp chứng mạng máy tính
- Kỹ thuật giấu thông tin (Steganography)
- Pháp chứng thiết bị di động & IoTs
- Thu thập thông tin OSINT
- Các kỹ thuật chống điều tra số
- … các chuyên đề thuyết trình

Quy định môn học

- Phương pháp: nghe giảng, đọc tài liệu (books, papers), thuyết trình (khi có yêu cầu), làm bài tập, …
- Lý thuyết: tham gia đầy đủ buổi học
- Vắng thi cuối kỳ (không lý do chính đáng): 0 điểm (~ không đạt môn học)

Quy định môn học

- Lưu ý:
  - Trễ deadline: trừ điểm tùy theo mức độ.
  - Trường hợp đặc biệt: trình bày với GV ngay từ đầu môn học, buổi học. Sau đó không giải quyết.

Đăng ký nhóm

- Nhóm 3-4 thành viên
- Đăng ký online, link xem trên moodle
- Hạn chót đăng ký: **12/3/2023**
- Sinh viên không đăng ký nhóm: 0 điểm quá trình.

Projects

- Đăng ký nhóm cần chú ý:
  - Thành viên nhóm có kiến thức nền tảng khác nhau, có cùng sở thích, … "**not just your friends**"
  - Các nhóm không làm cùng proj mà không có sự đồng ý của GV
- Ưu tiên nhóm đề xuất chủ đề thực hiện có nội dung liên quan đến môn học
- Danh sách đồ án gợi ý sẽ được công bố trên moodle môn học

Projects

- Yêu cầu báo cáo, đảm bảo các nội dung sau:
  - docx & pdf
  - pptx
  - video
  - Poster: A0
  - 10 câu hỏi trắc nghiệm (đưa vào phần phụ lục docx)
- Các mốc thời gian cụ thể: xem chi tiết trên moodle (dự kiến báo cáo từ tuần học thứ 12)

Projects

- **Mẫu poster A0:** tham khảo tại (khuyến khích sự sáng tạo về mẫu và nội dung, bố cục của poster):
  - https://sites.google.com/site/tuannguyenlatrobe/projects
  - https://drive.google.com/drive/folders/1njFIuwiM53RzBDYa8d2OH-sQPHNorosP?usp=sharing (login bằng tài khoản email SV)
  - https://khoahoctre.uit.edu.vn/trien-lam-khoa-hoc-cong-nghe-hoi-nghi-khoa-hoc-tre-va-nghien-cuu-sinh-nam-2021

Đánh giá (dự kiến)

- Quá trình: 30%
  - Chuyên cần
  - Đồ án
  - Bài tập/Challenge
- Thực hành: 30% (HT1)
- Cuối kỳ: 40% (TN+TL)

Tài liệu tham khảo

- CHFI - EC-Council's Certified Hacking Forensic Investigator
- William Oettinge (2020), Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence, Packt.
- FOR308: Digital Forensics Essentials, https://www.sans.org/cyber-security-courses/digital-forensics-essentials/ (Nov-2020)
- FOR526: Advanced Memory Forensics & Threat Detection, https://www.sans.org/cyber-security-courses/advanced-memory-forensics-and-threat-detection/ (Nov-2020)
- Forensics, https://trailofbits.github.io/ctf/forensics/ (Nov-2020)
- Windows Forensics, https://www.sans.org/cyber-security-courses/windows-forensic-analysis/ (Nov-2020)
- FOR518: Mac and iOS Forensic Analysis and Incident Response, https://www.sans.org/cyber-security-courses/mac-and-ios-forensic-analysis-and-incident-response/ (Nov-2020)
- FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response, https://www.sans.org/cyber-security-courses/advanced-network-forensics-threat-hunting-incident-response/ (Nov-2020)

Các công cụ sử dụng

- Sleuth Autopsy
- FTK Imager
- Wireshark
- Volatility
- …

Q&A

Câu hỏi chuẩn bị

1. Pháp chứng, pháp chứng số là gì?
2. Theo bạn, bạn đã từng làm pháp chứng số chưa? Nêu ví dụ cụ thể?
3. Theo bạn, điều kiện để các bằng chứng số được tìm thấy có giá trị cao, được công nhận là gì?

TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#0: Intro & Logictics
Spring 2023

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn